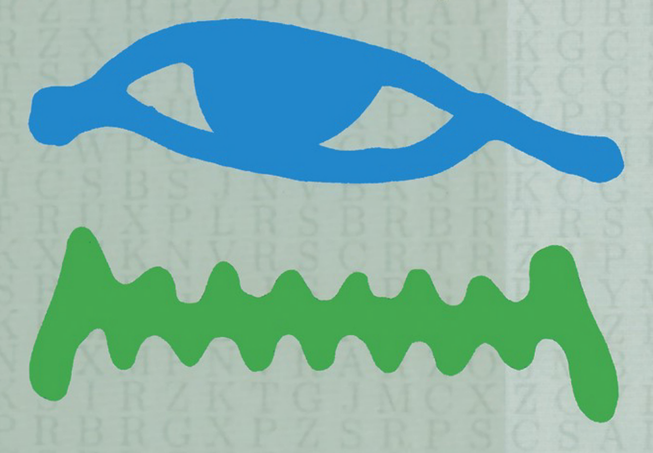
F. L. Bauer

Entzifferte Geheimnisse

Methoden und Maximen der Kryptologie

Dritte, überarbeitete und erweiterte Auflage





Springer

Entzifferte Geheimnisse

Springer
Berlin
Heidelberg
New York
Barcelona
Hongkong
London
Mailand
Paris
Singapur
Tokio

Friedrich L. Bauer

Entzifferte Geheimnisse

Methoden und Maximen der Kryptologie

Dritte, überarbeitete und erweiterte Auflage

Mit 166 Abbildungen, 26 Tabellen
und 16 Farbtafeln


Springer

Dr. rer. nat. Dr. ès sc. h.c. Dr. rer. nat. h.c. mult. Friedrich L. Bauer
Professor emeritus der Mathematik und Informatik
Technische Universität München
Institut für Informatik
Arcisstraße 21, 80333 München
Deutschland

ACM Computing Classification (1998): E.3, D.4.6, K.6.5, E.4
Mathematics Subject Classification (1991): 94A60, 68P25

ISBN 3-540-67931-6 Springer-Verlag Berlin Heidelberg New York
ISBN 3-540-62632-8 2. Auflage Springer-Verlag Berlin Heidelberg New York

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Bauer, Friedrich L.: Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie / Friedrich L. Bauer. – 3., überarb. u. erw. Aufl. – Berlin; Heidelberg; New York; Barcelona; Hongkong; London; Mailand; Paris; Singapur; Tokio: Springer, 2000
ISBN 3-540-67931-6

Springer-Verlag Berlin Heidelberg New York
Ein Unternehmen der BertelsmannSpringer Science+Business Media GmbH

Umschlaggestaltung: *design & production* GmbH, Heidelberg
Farbaufnahmen: Reinhard Krause, Deutsches Museum München
Satz: Vom Autor in TEX

Gedruckt auf säurefreiem Papier SPIN 10777934 45/3142 ud – 5 4 3 2 1 0

Vorwort

Gegen Ende der sechziger Jahre begann, unter dem Einfluß der raschen Entwicklung der Mikroelektronik, die Kryptologie aus ihrem verborgenen Dasein herauszutreten. Unter den Informatikern wuchs das Interesse an ihr. Damals konnte ich das Fehlen einschlägiger Kenntnisse (bei den meisten Informatikern) über die lange Entwicklung und den hohen Stand der professionellen Kryptologie beobachten. Ich befürchtete, daß dies nachteilig für die kommerzielle und wissenschaftliche Entwicklung sein würde und daß die amtlichen Dienste in einer Vorteilsposition waren, die sie auch ausnützen würden.

So kam ich auf den Gedanken, an der Technischen Universität München Vorlesungen über dieses Thema zu halten. Gestützt vornehmlich auf das reichhaltige und zuverlässige Buch "The Codebreakers" (1967) von *David Kahn*, fanden sie erstmals 1977/78, sowie dann 1981 (unter Mitarbeit von *Manfred Broy*), 1986/87 (unter Mitarbeit von *Herbert Ehler*) und seit 1990/91 wiederholt (unter Mitarbeit von *Anton Gerold*) statt. Seit 1995 hat Herr *Dr. Gerold* einen Lehrauftrag für das Gebiet an der Technischen Universität München.

Die Vorlesung im Wintersemester 1977/78 war ein Versuchsballon. Ich kündigte sie deshalb an als ‚Spezielle Probleme der Informationstheorie' und war damit sicher, daß weder zu viele Studenten noch Interessenten von außerhalb der Universität kommen würden. Im Sommersemester 1981 kündigte ich eine Vorlesung unter dem offenen Titel ‚Kryptologie' an. Es war sicher die erste öffentliche Vorlesung über dieses Thema an einer deutschen, wenn nicht sogar an einer kontinentaleuropäischen Universität[1].

Ich hielt es für gut möglich, daß die amtlichen Dienste aufmerksam würden; allerdings hatte ich keine Ahnung, wie schnell und in welcher Art und Weise sie sich bemerkbar machen würden. Es geschah nichts. Als ich dann im Wintersemester 1986/87 die Vorlesung wieder hielt, sagte ich trotzdem in der ersten Stunde, als ich über den „heimlichen" (*clandestine*) Charakter der Kryptologie sprach, scherzend zu meinen Studenten: „Wenn Sie eines Tages in der Vorlesung die Ihnen bisher unbekannten Gesichter zweier mittelal-

---

[1] *A. Konheim* wurde 1978 durch *J. Schwartz* aufgefordert, eine einsemestrige Vorlesung über kryptographische Methoden am Courant Institute der New York University zu halten.

terlicher Herren mit Anzügen, die sich von den Ihren abheben, bemerken sollten, so denken Sie sich etwas.“ Wie es der Zufall wollte, platzten nach etwa sechs Wochen zwei Gestalten, auf die meine Beschreibung paßte, in die Vorlesung – eine Viertelstunde nach Beginn; aber der Seminarraum 1229, in dem sie stattfand, ist schwer zu finden. Geistesgegenwärtig begrüßte ich sie mit: „Grüß Gott, die Herren, kommen's direkt aus Pullach?“ Großes Gelächter bei den Studenten und verlegene Gesichter bei den beiden, die mir eine Antwort schuldig blieben. So weiß ich bis heute nicht, ob mein Verdacht gerechtfertigt war. Ich wiege mich weiterhin in der Hoffnung, daß meine Tätigkeit die amtlichen Dienste nicht stört.

Aus der Vorlesung 1986/87 entstand dann sogar ein Skriptum. Das Drängen der Studierenden nach einer regelmäßigen Kryptologie-Vorlesung wurde dadurch vielleicht sogar verstärkt, und so kam es nach meiner Emeritierung noch zur Vorlesung 1990/91 und zu einer um die Kryptanalyse erweiterten, die ich im Sommersemester 1993 und Wintersemester 1993/94 abhielt. Das nunmehr durch die Kryptanalyse ergänzte Skriptum führte dann zu einem Studienbuch, das in erster Auflage 1993, in zweiter 1994 erschien. Eine Ausgabe mit festem Einband wurde erweitert und gründlich überarbeitet. Sie wurde möglich durch das rege Interesse, das das Buch auch außerhalb der Fachwelt gefunden hat. Die vorliegende dritte Auflage, die zu der englischen Ausgabe parallel läuft, wurde wiederum überarbeitet und erweitert.

Ich habe insbesondere versucht, auf den nichtmathematischen Leser Rücksicht zu nehmen. In einer lobenden Besprechung des Buches schrieb *Thomas von Randow* in der ZEIT: „... daß der Text in dem Maße, in dem er sich den Verfahren der modernen Wissenschaft nähert, an Trockenheit zunimmt. So werden die meisten Leser, die Kryptologie nicht studieren müssen, ... die Lektüre vorzeitig beenden. Dennoch wird niemand den Kauf bereuen. Geraten sei allerdings jenen, die den ersten Buchteil nicht bis zur Neige ausschöpfen möchten oder können, mit dem zweiten Teil ‚Kryptanalyse‘ erneut zu beginnen. Dort findet sich nicht nur viel Leichtverständliches, ... sondern auch Anregendes.“ Diese den Kern treffende Anregung soll dem Leser des Buches nicht vorenthalten werden. Die Kryptanalyse bietet in der Tat eine Fülle vergnüglicher Einzelheiten. Das Ganze muß jedoch auf die inneren Zusammenhänge hin ausgerichtet werden, und dafür ermöglicht der mathematische Formalismus die kürzeste und auch klarste Darstellung. Die nach Mathematik riechenden Einsprengsel mag mancher Leser auch überschlagen, zumindest bei der ersten Lektüre; er wird dann auf sie zurückgreifen können, wenn er gewisse Einzelheiten genauer oder auch ganz genau verstehen will. Im übrigen ist die verwendete Mathematik ganz elementar und liegt im Stoffumfang der Oberstufe des Gymnasiums.

Ich bin es dem Leser nun doch schuldig, zu erklären, wo mein Interesse an der Kryptologie und meine Vertrautheit mit ihr herrührt. Vorab, mein größter Vorteil ist, daß ich nie Angehöriger eines Dienstes war. Ich stehe also unter keiner irgendwie gearteten Schweigepflicht. Wohl konnte ich jedoch

meine Augen offenhalten und meine Ohren gebrauchen; mein wissenschaftliches Metier war auch ein günstiger Ausgangspunkt für mancherlei Gespräche. Trotzdem weiß ich nie, ob ich das, was ich weiß, auch wissen darf. Jedoch fing es zunächst ganz harmlos an: 1951 erzählte ich *Wilhelm Britzelmayr*, meinem damaligen Logikprofessor an der Ludwig-Maximilians-Universität München, von meiner Erfindung eines fehlerkorrigierenden Codes für Fernschreibverbindungen[2]. Das löste bei ihm eine falsche Assoziation aus, und er gab mir ein paar Tage darauf ein Exemplar des eben erschienenen Buches von *Sacco*[3]. Ich hatte insofern Glück, als es das beste Buch war, das ich damals bekommen konnte – was ich allerdings nicht wußte –, und ich verschlang es. Von da an kam ich von der Kryptologie nicht mehr los. Zudem legte mir mein Mitassistent und (fast väterlicher) Freund *Paul August Mann*, der von meinem Interesse an *Shannons* Arbeiten über redundanzmindernde Codierung wußte, eines Tages im Jahr 1951 die inzwischen berühmte, aber damals als Bell System Technical Report nur schwer zugängliche Arbeit von *Claude Shannon* "Communication Theory of Secrecy Systems" auf den Tisch[4]. Ich war fasziniert von diesem Hintergrund der mir bereits geläufigen mathematischen Informationstheorie *Shannons*. Dies prägte mein Interesse für Kryptologie, aufgefaßt als Seitengebiet der Theorie der Codierung und der formalen Sprachen im weitesten Sinn – einem Gebiet, das mich lange Jahre wissenschaftlich beschäftigte. In den frühen fünfziger Jahren wurde mir dann von meinem Chef *Robert Sauer* der Entwurf einer Dissertation „Hilfsgeräte der Kryptographie" von Postrat Dipl.-Ing. *Willi Jensen* (Flensburg) mit der Bitte um Begutachtung vorgelegt. Diese sehr aufschlußreiche Arbeit wurde nicht veröffentlicht. Merkwürdige Zufälle – oder vielleicht geschärfte Aufmerksamkeit – führten mich dann immer wieder zu Berührungen mit Persönlichkeiten, die der Kryptologie näher standen: mit *Karl Stein* (München) 1955, mit meinem Mainzer Kollegen *Hans Rohrbach* 1959, mit *Helmut Grunsky* und *Ernst Witt*. Auch mit *Erich Hüttenhain* (Bad Godesberg) wurde ich 1957 bekannt; unsere Gespräche über maschinelle Kryptologie konnten aber den Umständen gemäß in gewisse Details nicht gehen. Unter den amerikanischen und britischen Berufskollegen, mit denen ich engeren wissenschaftlichen Kontakt hatte, waren sicher einige, die im 2. Weltkrieg der Kryptologie nahestanden; doch darüber „sprach man nicht", insbesondere nicht vor 1976, dem Jahr, in dem auf einem Symposium in Los Alamos *B. Randell* und *I. J. Good* erste Einzelheiten aufdeckten. Kerngegenstand meines Interesses war jedenfalls, meinem wissenschaftlichen Metier entsprechend, über all die Jahre hinweg die ‚maschinelle Kryptanalyse'. Andere wichtige Apekte von SIGINT, wie 'traffic analysis' und 'direction finding', liegen nicht in der Reichweite dieses Buches, ebensowenig physikalische Maßnahmen zur Abschirmung der von Chiffriermaschinen ausgehenden elektromagnetischen Strahlung.

---

[2] DBP Nr. 892767, angemeldet 21. Januar 1951.
[3] *Général Luigi Sacco*, Manuel de Cryptographie. Payot, Paris 1951.
[4] Bell Systems Technical Journal **28**, Oct. 1949, p. 656–715.

Dieses Buch enthält im ersten Teil die krypto*graphischen* Methoden. Über Krypt*analyse* bringt es im zweiten Teil vor allem Hinweise, die für die Verfahrensbeurteilung wichtig sind und den Benutzer kryptographischer Methoden vor unliebsamen Überraschungen bewahren sollen. Eingedenk der Maxime von *Kerckhoffs* bemühte ich mich stets, meinen Studierenden auch grundlegende Erfahrungen in der Kryptanalyse zu vermitteln. Eine theoretische Vorlesung über bloße Methoden erschien mir blutleer. Hier sind aber Grenzen zu beachten: Der Spaß, den der neugierige Student zunächst an der unbefugten Entzifferung hat, könnte ihn vergessen lassen, daß professionelle Kryptanalyse ein hartes Geschäft ist. Auch kann man ihm keinen Höchstleistungsrechner wie CRAY unbeschränkt zur Verfügung stellen – es ist aber erstaunlich, wie viel man schon mit einem Arbeitsplatzrechner machen kann. Bedrückend ist, daß die amtlichen Dienste ein solches Unternehmen entweder als uninteressant einstufen müssen – wozu sollte man sich dann die Mühe machen – oder als gefährlich (‘*sensitive*’); es gibt kaum Spielraum dazwischen.

Meine intellektuelle Freude an der maschinellen Kryptologie konnte ich dann ab 1984 so richtig ausleben beim Aufbau des kryptologischen Kabinetts in der von mir konzipierten, 1988 eröffneten Sammlung „Informatik“ des Deutschen Museums München. Der Besuch der Ausstellung sei dem Leser wärmstens empfohlen. Mit freundlicher Genehmigung der Generaldirektion ist im Anhang der einschlägige Ausschnitt aus dem aktualisierten Führer durch die Ausstellung „Informatik“ abgedruckt.

Mein herzlicher Dank geht auch an die Herren *Manfred Broy*, *Herbert Ehler*, *Anton Gerold* und *Hugh Casement* (München), die mir in vielerlei Weise behilflich waren; den Herren *Karl Stein*, *Otto Leiberich*, *Ralph Erskine*, *Frode Weierud*, *Heinz Ulbricht*, *Tony Sale*, *Kjell-Ove Widman*, *Otto J. Horak* und *Fritz-Rudolf Güntsch* danke ich für anregende Gespräche und informativen Briefwechsel. Dem Deutschen Museum in München sei überdies gedankt für die Überlassung der von Herrn *Reinhard Krause* angefertigten Farbaufnahmen. Bei der Beschaffung weiterer Bildvorlagen und schwer zugänglicher Literatur kam mir auch die Hilfe der Crypto AG, Zug (Schweiz) sehr gelegen. Meinen besonderen Dank möchte ich abstatten Herrn *Kirk H. Kirchhofer*, Oberägeri. Dr. *Hildegard Bauer-Vogg* half mir bei den Korrekturen und bei der Übersetzung schwieriger lateinischer Texte, *Martin Bauer*, *Ulrich Bauer* und *Bernhard Bauer* lieferten Zeichnungen und Berechnungen; auch ihnen sei gedankt.

Herrn *J. Andrew Ross*, dem *copy editor* der englischen Ausgabe, verdanke ich zahlreiche Hinweise auf klärungsbedürftige Punkte im deutschen Text. Herr Dr. *Hans Wössner* vom Springer-Verlag war mir in vieler Weise behilflich; ihm danke ich wieder einmal für die gute Zusammenarbeit und für die reiche Ausstattung des Buches.

Grafrath, Sommer 2000 F. L. Bauer

Inhaltsverzeichnis

Farbtafeln

Teil I: Kryptographie

'ars ipsi secreta magistro'
[Eine selbst einem Meister verborgene Kunst]
Jean Robert du Carlet, 1644

„Der Schutz sensibler Information ist ein Anliegen,
das bis in die Anfänge menschlicher Kultur reicht“
Otto Horak, 1994

„„Denn es ist besser für den Schreiber, sich als Dummkopf ansehen zu lassen,
als den Preis für die Aufdeckung seiner Pläne zu bezahlen“
Giovanni Battista Porta, 1563



Giovanni Battista Porta
(1535–1615)

Die Leute


W. F. Friedman


M. Rejewski


A. M. Turing

Vor wenigen Jahren noch war die Kryptologie, die Lehre von den Geheimschriften und ihrer unbefugten Entzifferung, ein recht im Verborgenen blühender Zweig – blühend, weil von alters her ihre professionellen Vertreter gut ernährend. Denn die Kryptologie ist eine echte ‚Wissenschaft': Es geht um Wissen, um erfahrenes (‚tradiertes') ebenso wie um erprobtes.

Ihrer Natur nach handelt sie nicht nur von Geheimschriften, sondern bleibt auch selbst etwas im Geheimen – gelegentlich auch im Obskuren. Sie ist fast eine Geheimwissenschaft. Die klassische offene Literatur ist spärlich und schwierig aufzufinden: Mit dem Aufkommen allmächtiger Staatsgewalten müssen sich die professionellen Kryptologen in diplomatischen und militärischen Diensten weitgehend in die Anonymität begeben oder doch wenigstens eine Zensur ihrer Veröffentlichungen hinnehmen. Dementsprechend gab die offene Literatur nie völlig den Wissensstand wieder – man darf annehmen, daß es heute nicht anders ist.

Verschiedene Länder sind dabei unterschiedlich zurückhaltend: Während die Vereinigten Staaten von Amerika – wen wundert das – recht großzügig einige Informationen über die Situation im 2. Weltkrieg herausließen, hüllte sich die damalige Sowjetunion in Schweigen. Aber auch Großbritannien pflegt eine Geheimniskrämerei, die manchmal – so in der Sache 'COLOSSUS' – unangemessen erscheint. Lediglich über den Stand der Kryptologie im Deutschen Reich wurde nach dem Zusammenbruch 1945 offen berichtet.[1]

Die Kryptologie ist eine Jahrtausende alte Wissenschaft. Ihre Entwicklung stand mit der Entwicklung der Mathematik zumindest personell gelegentlich in Berührung – Namen berühmter Leute wie *François Viète* (1540–1603) und *John Wallis* (1616–1703) tauchen auf. In einer modernen mathematischen Betrachtungsweise zeigt sie statistische (*William F. Friedman*, 1920), algebraisch-kombinatorische (*Lester S. Hill*, 1929) und stochastische Züge (*Claude E. Shannon*, 1941).

---

[1] *Hans Rohrbach*, Mathematische und maschinelle Methoden beim Chiffrieren und Dechiffrieren. In: FIAT Review of German Science 1939–1941: Applied Mathematics, Part I, Wiesbaden 1948.

Der 2. Weltkrieg brachte endgültig die Mathematiker an die kryptologische Front: Beispielsweise standen sich gegenüber *Hans Rohrbach* (1903–1993) in Deutschland,[2] *Alan Turing* (1912–1954) in England;[3] in den USA waren *A. Adrian Albert* (∗ 1905) und *Marshall Hall* (1910–1990) engagiert,[4] in Polen *Marian Rejewski* (1905–1980), in Schweden *Arne Beurling* (1905–1986), in Norwegen *Ernst S. Selmer* (∗ 1920), in den Niederlanden *Maurits de Vries*.

Mathematische Disziplinen, die nach dem heutigen Stand für die Kryptologie von Belang sind, umfassen unter anderem: Zahlentheorie, Gruppentheorie, Kombinatorik, Relationentheorie, Komplexitätstheorie, Ergodentheorie, Informationstheorie. „Das Schlüssel- und Entzifferungswesen ist bereits praktisch als Untergebiet der Angewandten Mathematik anzusehen“ *(Kirk H. Kirchhofer)*. Für den Informatiker gewinnt die Kryptologie zusehends praktische Bedeutung, mehr und mehr gebraucht der Kryptologe die Informatik.

Man kennt also die Namen einiger Mathematiker der neueren Zeit, die kürzere oder längere Zeit kryptologisch tätig waren. Im allgemeinen ist es aber verständlich, wenn hoheitliche Geheimdienste selbst die Namen führender Kryptologen nicht der Öffentlichkeit preisgeben.[5] Zu sehr lebt die professionelle Kryptologie unter den Gefahren nachrichtendienstlicher Bemühungen. Es ist bedeutsam, den potentiellen Gegner über die eigenen Ansichten zur Auswahl von Verfahren (die ‚Chiffrierphilosophie‘) ebenso im unklaren zu lassen wie über die eigenen Fähigkeiten zum unbefugten Entziffern. Gelingt aber eine unbefugte Entzifferung – den Engländern gelang sie 1940 für die ENIGMA-Chiffrierung –, so ist es wichtig, diesen Sachverhalt vor dem Gegner zu verbergen und sich nicht durch Reaktionen zu verraten. So blieben infolge britischer Klugheit die maßgeblichen deutschen Stellen bis 1944

---

[2] Eine nennenswerte Anzahl bekannter deutscher Mathematiker könnte hier aufgelistet werden, darunter *Georg Hamel* (1877–1954), Hans Rohrbach (1903–1993), *Wolfgang Franz* (1905–1996), *Karl Stein* (∗ 1913), *Helmut Grunsky* (1904–1986), *Gottfried Köthe* (1905–1989), *Ernst Witt* (1911–1991), *Theodor Kaluza* (1910–1994), *Gisbert Hasenjäger* (∗ 1919), zeitweilig (Mitte 1941–Mitte 1943) auch der geniale, aber als fanatischer Nazi mit Aktionen gegen *Landau* und *Courant* unrühmlich hervorgetretene *Oswald Teichmüller* (1913–1943).

[3] Auch in Großbritannien wurden im 2. Weltkrieg zahlreiche Mathematiker rekrutiert, darunter *Maxwell Herman Alexander Newman* (1897–1984), *Gordon Welchman* (1906–1985), sowie *Peter Hilton*, *Shaun Wylie*, *Dennis W. Babbage*, *J. H. C. (Henry) Whitehead*, *Donald Michie*, *Rolf Noskwith*, *William Thomas Tutte*, und einige Schachmeister, darunter *Hugh Alexander*, *Stuart Milner-Barry* und *Harry Golombek*.

[4] sowie *Howard T. Engstrom*, *Andrew M. Gleason*, die Logiker *J. Barkley Rosser*, *Willard Van Orman Quine* und die Angewandten Mathematiker *Vannevar Bush*, *Warren Weaver*.

[5] *Admiral H. P. F. Sinclair*, der 1923 Chef des britischen Entzifferungsdienstes wurde, war unter seinem Spitznamen ‘Quex’ bekannt. Offiziös wurde er, wie auch sein Nachfolger *General Sir Stewart Graham Menzies* (1890–1968), im 2. Weltkrieg Chef des *British Secret Intelligence Service* (M.I.6), damals allgemein nur mit "C" bezeichnet. "C" herrschte über eine größere Anzahl von ‘Passport Control Officers’, die an den Botschaften tätig waren, ebenso wie über die kryptanalytische Truppe in Bletchley Park. Und der Name von *Ernst C. Fetterlein* (–1944), der dem Zaren bis 1918 als Chef des Entzifferungsbüros diente und seit den 20er Jahren im Dienst der *Government Code and Cypher School* des *Foreign Office* stand, wurde erst 1985 von *Christopher Andrew* und 1986 von *Nigel West* in der offenen kryptologischen Literatur erwähnt. *Andrew Hodges* schreibt sogar (vermutlich Hörfehler) den Namen falsch: *Feterlain*.

(und einige einsichtslose Leute bis 1974) überzeugt, die Chiffrierung ‚ihrer' ENIGMA-Maschine sei nicht zu brechen.

Die Vorsicht der Alliierten ging so weit, daß sie auch Desinformation der eigenen Leute einkalkulierten: Capt. *L. F. Safford*, U.S. Navy, Office of Naval Communications, Cryptography Section schrieb in einem internen Bericht vom 18. März 1942, nach Rückkehr von Capt. *A. Sinkov* und Lt. *L. Rosen* im Februar 1941 von einer informativen Reise zu den Briten, ignorant oder wider besseres Wissen: "Our prospects of ever breaking the German 'Enigma' cipher machine are rather poor". Der Bericht war allerdings in erster Linie an seine Untergebenen in OP-20-G der U.S. Navy gerichtet.

Im Krieg müssen Material und sogar Menschen geopfert werden, um anderweitig größere Verluste zu ersparen. In England gab es nach dem Krieg einige Diskussionen darüber, ob die Bombardierung von Coventry im November 1940 durch Mitlesen des ENIGMA-chiffrierten Funkverkehrs der deutschen Kampfgruppe 100 hätte abgewendet werden können. Da die Angriffsziele mit Zahlen bezeichnet wurden, war dies in der Tat nicht möglich. Jedoch waren die Briten zunächst sehr bestürzt, als die Amerikaner Mitte 1943 begannen, alle Tanker-U-Boote zu vernichten, deren Positionen sie durch den inzwischen geglückten Bruch der 4-Rotoren-ENIGMA im Netz des Oberbefehlshabers der U-Boote erfuhren. Sie waren zu Recht besorgt, daß die Deutschen Verdacht schöpfen und ihr ENIGMA-System wieder ändern könnten – sie taten es nicht, sondern führten die Verluste fälschlicherweise auf Verrat zurück. Wie berechtigt die Sorge der Alliierten war, zeigte sich, als sie erfuhren, daß die Kriegsmarine ab 1. Mai 1945 eine Änderung des Chiffrierverfahrens vorbereitet hatte, die alle bisherigen Entzifferungsmethoden zunichte gemacht hätte. "This change could probably have been implemented much earlier if it had deemed worthwhile" (*Ralph Erskine*).

Dieses Meisterstück von Gewährleistung der Sicherheit der Nachrichtenbeschaffung wurde offiziell "intelligence resulting from the solution of high-grade codes and ciphers" genannt, kurz "Special Intelligence", britischer Deckname ULTRA. Die U.S.-Amerikaner nannten MAGIC die Informationen, die sie aus dem Einblick in die japanische PURPLE-Chiffrierung erzielten. ULTRA wie MAGIC entgingen den Spionen der Achsenmächte.

Berührung hat die Kryptologie auch mit der Kriminalistik. Hinweise auf kryptographische Methoden finden sich in einigen Lehrbüchern der Kriminalistik, meist begleitet von Berichten über geglückte Entzifferung der Botschaften von noch nicht gefaßten Verbrechern – Schmugglern, Rauschgifthändlern, Schiebern, Erpressern, Wettbetrügern – und von bereits einsitzenden, denen es um Geldbeschaffung, Ausbruchspläne und Zeugenbeeinflussung geht. Vor Gericht mag für die Überführung der Angeklagten das Gutachten von Kryptologen ausschlaggebend sein. Hierin erwarb sich zur Zeit der Prohibition in den U.S.A. besondere Verdienste Mrs. *E. S. Friedman* (1892–1980), die Frau des berühmten Kryptologen *William Frederick Friedman* (1891–

1969)[6] und selbst eine professionelle Kryptologin. Sie hatte es vor Gericht nicht immer leicht; die Verteidigung versuchte einmal darzulegen, daß man aus einer Geheimschrift alles herauslesen könne und daß ihre Entzifferung nichts als *"an opinion"* sei. Auch der schwedische Kryptologe *Yves Gyldén* (1895–1963), ein Enkel des Astronomen *Hugo Gyldén*), half 1934 der Polizei, Schmuggler einzufangen. Nur wenige Kriminal-Kryptologen werden bekannt, wie der Wiener *Siegfried Türkel* mit einem Buch 1927 oder *Abraham P. Chess* aus New York anfangs der fünfziger Jahre. Neuerdings hat die sich ausbreitende, kryptographische Methoden verwendende internationale Kriminalität begonnen, die besondere Aufmerksamkeit der Kryptanalysis zu erwecken.

Neben der staatlichen Kryptologie in Diplomatie und Militär steht insbesondere seit dem Beginn der Aufklärung die amateurhafte. Angefangen von der Aufdeckung historischer Begebenheiten durch pensionierte Professionelle wie *Étienne Bazeries*[7] bis zum Salonvergnügen, dem sich *Wheatstone*[8] und *Babbage*[9] widmeten, mit journalistischem Hintergrund von *Edgar Allan Poe* bis zum *Cryptoquip* der heutigen Los Angeles Times, mit Ausblicken auf Okkultismus, Marsmännchen und Terrorismus, bietet sich ein bunter Teppich, durchsetzt mit Geschichten aus einer der ältesten Sparten der Kryptographie, dem Austausch geheimer Botschaften zwischen Liebenden.



Die um die Mitte des 18. Jahrhunderts aufkommenden Briefsteller bieten bald auch kryptographische Hilfsmittel an, so *Allzeitfertiger Briefsteller* von Chrysostomus Erdmann Schröter, Leipzig 1743 und *Ganz neu entdecktes Kunststück so geheim zu schreiben, dass es kein Dechiffreur auflösen kann* von einem C. W. P., Ulm 1764, oder *De geheime brieven-schryver, angetoond met verscheydene voorbeelden* von einem G. v. K., Amsterdam 1780, auch *Der zauberische Schreibekünstler* von einem Anonymus, Leipzig 1795, ähnlich *Dem Magiske skrivekunstner*, Kopenhagen 1796; etwas nüchterner *On an easy and secure Method of Secret Correspondence* von einem "B" im *Quarterly Journal of Science*, 1822 und ganz unverblümt *Trésor des Amans* von J.-P.-A. Lacrouts, Paris 1834. Solcherart Titel, bald angereichert mit Hinweisen auf Stenographie und Telegraphie, setzen sich fort bis ins 20. Jahrhundert, besonders hübsch *Sicherster Schutz des Briefgeheimnisses* von Emil Katz,

6 Der wohl bedeutendste U.S.-amerikanische Kryptologe unserer Zeit. Er führte 1920 mit dem *Index of Coincidence* die schärfste Waffe der modernen Kryptanalysis ein.

7 *Étienne Bazeries* (1846–1931), wohl der vielseitigste französische Kryptologe gegen Ende des 19. Jahrhunderts, Verfasser des Buches ≪Les chiffres secrets dévoilés≫ (1901).

8 *Charles Wheatstone* (1802–1875), englischer Physiker (‚Wheatstone'sche Brücke').

9 *Charles Babbage* (1791–1871), englischer Gelehrter, am bekanntesten durch seine beiden Maschinen *'Difference Engine'* und *'Analytical Engine'*.

Berlin 1901 und *Amor als geheimer Bote. Geheimsprache für Liebende zu Ansichts-Postkarten*, vermutlich von Karl Peters, Mülheim 1904.

Ihrer abwechslungsreichen Anzüglichkeiten wegen ist die Historie der Kryptologie besonders vergnüglich zu studieren. Vermischt mit sensationsbehafteten Details aus dem 1. und 2. Weltkrieg, trat ein solches spannendes Bild der Kryptologie in kompakter Form erstmals einer breiten Öffentlichkeit entgegen in *David Kahn*s journalistischer wie auch historischer Meisterleistung "The Codebreakers" von 1967. Ende der siebziger Jahre folgten einige Ergänzungen aus inzwischen freigegebener britischer Sicht, insbesondere von *Frederick W. Winterbotham*, *Patrick Beesley*, *Brian Johnson* und *Gordon Welchman*, die insbesondere die ernste Seite der Kryptologie beleuchten.

Das kommerzielle Interesse an Kryptologie war nach der Erfindung des Telegraphen auf die Produktion von Codebüchern und etwa seit Anfang des Jahrhunderts auf die Konstruktion von mechanischen und elektromechanischen Chiffriermaschinen konzentriert. Elektronische Rechenanlagen wurden in Weiterführung der Ansätze aus dem 2. Weltkrieg schon bald zum Brechen von Kryptogrammen eingesetzt. Als Chiffriermaschine genügt durchaus ein programmierbarer Taschenrechner. Aber erst um die Mitte der siebziger Jahre wurde ein weitverbreitetes kommerzielles Interesse an der Chiffrierung von privaten Nachrichtenkanälen manifest, wobei die Möglichkeiten, die mikrominiaturisierte Schaltungen (‚Chips') bieten, mit den Notwendigkeiten, die in rechnergestützten Nachrichtensystemen ('*electronic mail*') auftraten, zusammentrafen. Ein weiteres tat die Verunsicherung, die allerorten durch Gesetze zum Datenschutz einerseits, durch Skandalmeldungen über angezapfte Verbindungen (einschließlich Richtmikrophone und Aufzeichnung elektromagnetischer Abstrahlung) oder breitflächige Industriespionage andererseits hervorgerufen wurde. Ein gesteigertes Bedürfnis nach Informationsschutz trieb die Bedeutung der Kryptologie in früher kaum vorstellbare Höhen. So sind plötzlich private, kommerzielle Anwendungen der Kryptologie in den Vordergrund gerückt. Sie zeigen dabei einige nichtorthodoxe Betriebsweisen, insbesondere die von *Whitfield Diffie* und *Martin Hellman* 1976 erfundenen unsymmetrischen ‚öffentlichen' Schlüsselsysteme.

Das Fehlen ausreichenden Quellenschutzes für Programme legt den Einsatz von Chiffriermethoden für kommerzielle Software besonders nahe.

„Kryptologie für jedermann" (*public cryptography*) tritt aber als eine in sich widersprüchliche Forderung auf und führt zu einem Interessenkonflikt der Staatsmacht mit der Wissenschaft. Eine Beschäftigung zahlreicher Wissenschaftler mit diesem Gebiet wirft in den Großstaaten Probleme der nationalen Sicherheit auf. Bezeichnenderweise begann man zuerst in den Vereinigten Staaten darüber nachzudenken, ob nicht ein Verbot der privaten Forschung auf dem Gebiet der Kryptologie – entsprechend dem bestehenden Verbot der privaten Forschung auf dem Gebiet der nuklearen Waffen – erlassen werden sollte. Am 11. Mai 1978 – zwei Jahre nach der revolutionären Erfindung von *Diffie* und *Hellman* – schrieb ein hoher Justizbeamter, *John M. Har-*

mon, Assistant Attorney General, Office of Legal Counsel, an *Dr. Frank Press*, Science Advisor to the President "*The cryptographic research and development of scientists and mathematicians in the private sector is known as 'public cryptography'. As you know, the serious concern expressed by the academic community over government controls of public cryptography led the Senate Select Committee on Intelligence to conduct a recently concluded study of certain aspects of the field*". Diese Umstände betrafen u.a. die Frage, ob Einschränkungen aufgrund der *International Traffic in Arms Regulation* (ITAR) "*on dissemination of cryptographic information developed independent of government supervision or support by scientists and mathematicians in the private sector*" unter der Verfassung der U.S.A. ('First Amendment: Freedom of Speech, of the Press etc.') zulässig seien.

Es wird festgestellt: "*Cryptography is a highly specialized field with an audience limited to a fairly select group of scientists and mathematicians ... a temporary delay in communicating the results of or ideas about cryptographic research therefore would probably not deprive the subsequent publication of its full impact. Cryptographic information is both vital and vulnerable to an almost unique degree. Once cryptographic information is disclosed, the damage to the government's interest in protecting national security is done and may not be cured.*". Damit wird "*a licensing scheme requiring prepublication submission of cryptographic information*" für zulässig erklärt, "*a prepublication reviews requirement for cryptographic information, if it provided necessary procedural safeguards and precisely drawn guidelines*". Ein Verbot der privaten Forschung ("*a prior restraint on disclosure of cryptographic ideas and information developed by scientists and mathematicians in the private sector*") sei jedoch verfassungswidrig. In den achtziger Jahren wurde auf die Brisanz des Problems wiederholt hingewiesen, das Justizministerium warnte: "*export controls on cryptography present sensitive constitutional issues*".

Man muß den Dingen ins Gesicht sehen: Kryptosysteme werden nicht nur von der U.S. Regierung als Waffen angesehen, Kryptosysteme sind Waffen – sowohl Verteidigungswaffen wie auch Angriffswaffen. Wem das nicht klar ist, der hat aus dem Verlauf des 2. Weltkriegs nichts gelernt.

Harmon schrieb ferner: "*Atomic energy research is similar in a number of ways to cryptographic research. Development in both fields has been dominated by government. The results of government created or sponsored research in both fields have been automatically classified because of the imminent danger to security flowing from disclosure. Yet meaningful research in the field may be done without access to government information. The results of both atomic energy and cryptographic research have significant nongovernmental uses in addition to military use. The principal difference between the fields is that many atomic energy researchers must depend upon the government to obtain radioactive source material necessary in their research. Cryptographers, however, need only obtain access to an adequate computer.*"

Mit anderen Worten: Mit Kryptologie ist gefährlicher Umgang noch leichter möglich als mit Atomenergie. Wenigstens tötet die Waffe CRYPTO nicht unmittelbar – wohl aber deckt sie auch Verbrechen.

Die Verantwortlichkeit von Regierung und Wissenschaft gegenüber der Leichtfüßigkeit kryptologischer Betätigung schlug sich nieder im *Computer Security Act* des *U.S.Congress* von 1987 (Public Law 100–235). Darin wurde ein *Computer System Security and Privacy Advisory Board* (CSSPAB) geschaffen, mit Mitgliedern aus der Regierung und aus der Computerindustrie. Obschon also ein latenter Konflikt vorlag, schien es sich in den USA bis 1993 zu bestätigen, daß sein Ausbruch durch freiwillige Selbstkontrolle der Wissenschaft (*Public Cryptography Study Group*) vermieden werden kann.

Danach brach jedoch ein *Crypto War* aus zwischen der Regierung der U.S.A. und Bürgerrechtsgruppen, die sich durch den, auch für das CSSPAB überraschend, im April 1993 angekündigten und im Februar 1994 veröffentlichten[10] *Escrowed Encryption Standard* (EES) herausgefordert fühlten. Er sieht eine Hinterlegungspflicht für Schlüssel vor. Anfang Januar 2000 scheint sich eine Entspannung für den Krypto-Export abzuzeichnen. Obschon dieser Konflikt auf einer anderen als der wissenschaftlichen Ebene, nämlich auf einer politischen, liegt, könnte er doch auch die Freiheit der Wissenschaft gefährden.

Im liberalen demokratischen Europa sieht es derzeit besser aus; es ist im Jahr 2000 nicht zu befürchten, daß die Regierungen Erfolg haben würden mit einer Einengung der Wissenschaft. In der Europäischen Union wurden allerdings 1994 erste Schritte unter dem Stichwort 'Euro-Encryption' gemacht, die auch zur Regelung des unausweichlichen Interessenkonfliktes der Staatsmacht mit der Wissenschaft führen könnten. 1999 führte Deutschland im weltweiten Liberalisierungstrend. Frankreich schaffte 1999 die staatliche Schlüsselhinterlegungspflicht ab. In der ehemaligen Sowjetunion wurde der Konflikt selbstverständlich im Rahmen des bestehenden Systems erledigt, aber heutigen Rußland wie in China und Israel herrscht weiterhin eine strenge nationale Überwachung.

Kryptographie und Kryptanalyse sind die zwei Gesichter der Kryptologie, die sich gegenseitig bedingen und beeinflussen, in einem Wechselspiel von Verbesserungen zur Erhöhung der kryptanalytischern Sicherheit einerseits und von Anstrengungen zu wirkungsvolleren Angriffen andrerseits. Erfolge sind ziemlich selten, Mißerfolge sind eher häufig. Die Schweigsamkeit der hoheitlichen Dienste hilft auch, ihre Niederlagen zu verbergen. Allen Großmächten des 2. Weltkriegs gelang es zumindest gelegentlich, ihre Gegner aufs Kreuz zu legen, alle hatten sie aber auch Einbrüche hinzunehmen. Im 21. Jahrhundert wird es nicht anders sein, wenn auch *Otto Leiberich* zuzustimmen ist, daß unsichere Chiffrierverfahren mehr und mehr aussterben werden. Die selbst beim Gebrauch sicherer Verfahren immer noch unausrottbare menschliche Dummheit und Sorglosigkeit wird jedoch weiterhin für Einbrüche sorgen.

---

[10] *Escrowed Encryption Standard* (EES), Federal Information Processing Standards Publication (FIPS PUB) 185, Febr. 9, 1994.

1 Einleitender Überblick

≪En cryptographie, aucune règle n'est absolue.≫
Étienne Bazeries, 1901

1.1 Kryptographie und Steganographie

Es ist zu unterscheiden zwischen Kryptographie und Steganographie. Der Ausdruck **Kryptographie** (engl. *cryptography*, frz. *cryptographie*) wurde als '*cryptographia*' für *secrecy in writing* 1641 von *John Wilkins*, neben *Wallis* einem der Gründer der *Royal Society*, eingeführt; *cryptography* verwendete 1658 der Arzt *Thomas Browne*. Die Methoden der Kryptographie machen eine Nachricht für den Unbefugten unlesbar, unverständlich – '*ars occulte scribendi*'. Im Deutschen spricht man auch von *offenen* (d.h. *offensichtlich* als solche erkennbaren) *Geheimschriften*, engl. *overt secret messages*.

Der Ausdruck **Steganographie** (engl. *steganography*, frz. *stéganographie*) wurde von *Caspar Schott*, einem Schüler von *Athanasius Kircher*, in dem Buchtitel *Schola steganographia*, Nürnberg 1665 auch für ‚Kryptographie' verwendet; er findet sich schon in dem von *Trithemius* 1499 begonnenen ersten, noch reichlich obskuren Werk *Steganographia* mit der Bedeutung ‚verdecktes Schreiben'. Die Methoden – '*ars sine secreti latentis suspicione scribendi*' – zielen darauf ab, die bloße Existenz einer Nachricht (wie immer sie auch abgefaßt ist) zu verbergen (engl. *conceal*) – *gedeckte Geheimschriften*, engl. *covert secret messages*. Um ein Tagebuch zu führen[1] oder um einem Boten zu verwehren, von einer Nachricht Kenntnis zu nehmen, sind kryptographische Methoden angebracht; um eine Nachricht durch Gefängnistore zu schmuggeln[2] , steganographische Methoden.

Die Steganographie zerfällt in zwei Branchen, die *linguistische* und die *technische*. Nur die erstere hat mit der Kryptographie innere Berührung. Die **technische Steganographie** ist rasch erledigt. Sie arbeitet seit *Plinius* mit Geheimtinten. Bis heute sind Zwiebelsaft und Milch beliebt und bewährt

---

[1] Von *Samuel Pepys* (1633–1703) bis *Alfred C. Kinsey* (1894–1956).

[2] Von *Sir John Trevanion* (Abb. 13) unter *Oliver Cromwell* bis zum französischen Bankräuber *Pastoure*, dessen Überführung *André Langie* beschrieb, und zum Rechtsanwalt und Stasi-Agenten *Klaus Croissant*, der die Baader-Meinhof Bande verteidigte. Der Terrorist *Christian Klar* verwendete eine Buchchiffre.

(Braunfärbung beim Erwärmen oder im UV-Licht). Andere klassische Requisiten sind doppelte Böden und hohle Absätze.

Von modernen Errungenschaften seien erwähnt: Schnelltelegraphie (engl. *spurts*) – Übertragung vorgespeicherten Morsecodes mit 20 Zeichen per Sekunde – sowie Frequenzbandpermutation bei Sprechfunk (engl. *scrambler*), heute auch kommerziell weit verbreitet. Im 2. Weltkrieg wurden ab März 1942 von der ‚Forschungsanstalt' der Deutschen Reichspost (Postrat Dipl.-Ing. *Vetterlein*) ungenügend gesicherte Funkferngespräche zwischen *Roosevelt* und *Churchill* abgehört und über *Schellenberg* an *Himmler* weitergeleitet, so eines am 29. Juli 1943, unmittelbar vor dem Waffenstillstand mit Italien.

Für schriftliche Nachrichten wurde revolutionierend die Mikrophotographie; das *microdot* von der Abmessung eines Fliegendrecks nimmt eine ganze Seite (DIN A 4) auf – eine grandiose Entwicklung, ausgehend vom Macrodot des *Histiæus*[3], der seinen Sklaven kahl schor, ihm die Nachricht auf die Kopfhaut schrieb und dann erst warten mußte, bis diesem das Haar wieder gewachsen war. Der russische Spion *Abel* stellte die Microdots auf spektroskopischem Filmmaterial her, das er unauffällig kaufen konnte. Sein Kollege *Lonsdale* versteckte die Microdots im Rücken gebundener Zeitschriften. Die im 2. Weltkrieg von deutschen Dienststellen verwendeten Microdots schließlich hatten gerade die Größe, um als Schreibmaschinenpunkt verwendet zu werden.

1.2 Semagramme

Die **linguistische Steganographie** kennt zwei Klassen von Tarnverfahren: entweder eine geheime Nachricht als unverfängliche, offen verständliche Nachricht erscheinen zu lassen (engl. *open code*) oder in (eventuell winzigen, aber) sichtbaren graphischen Details einer Schrift oder Zeichnung auszudrücken (**Semagramm**, engl. *semagram*). Die letztere Klasse ist vor allem bei Amateuren beliebt. Sie erfüllt allerdings viele Wünsche nicht. Zu verräterisch sind graphische Details einem wachsamen Auge. So hat der Einfall des jungen *Francis Bacon* (1561–1626), zwei Schriftarten (Abb. 1) zu verwenden (publiziert in der ersten englischen Übersetzung von *De augmentis scientiarum*, 1623), keine große praktische Bedeutung erlangt. (Für den Code s. 3.3.3.)

Abb. 1. *Francis Bacon*: Sichtbare Tarnung eines binären Codes ('biliteral cipher') mittels zweier verschiedener Schriftzeichen-Formen. Man beachte die beiden verschiedenen /e/ in *Manere*

[3] *Kahn* schreibt S. 81 *Histiaeus*, S. 780 *Histaeius* und im Register gar *Histaieus*. Wahrlich *ars occulte scribendi* !

Dieses steganographische Prinzip scheint zur selben Zeit auch in Paris bekannt gewesen zu sein und wird von *Vigenère* 1586 erwähnt. Es hat sich über die Jahrhunderte gut erhalten: Die jüngsten mir bekannten Verwendungen stammen angeblich von *van Wijngaarden* (kursive und aufrechte Punkte im ALGOL 68 Bericht).

In Königsberg i. Pr. gabelt sich der Pregel und umfließt eine Insel, die *Kneiphof* heißt. In den dreißiger Jahren des achtzehnten Jahrhunderts wurde das Problem gestellt, ob es wohl möglich wäre, in einem Spaziergang jede der sieben Königsberger Brücken genau einmal zu überschreiten.

Daß ein solcher Spaziergang unmöglich ist, war für L. EULER der Anlaß, mit seiner anno 1735 der Akademie der Wissenschaften in St. Petersburg vorgelegten Abhandlung *Solutio problematis ad geometriam situs pertinentis* (Commentarii Academiae Petropolitanae 8 (1741) 128-140) einen der ersten Beiträge zur Topologie zu liefern.

Das Problem besteht darin, im nachfolgend gezeichneten Graphen einen einfachen Kantenzug zu finden, der alle Kanten enthält. Dabei repräsentiert die Ecke vom Grad 5 den Kneiphof und die beiden Ecken vom Grad 2 die Krämerbrücke sowie die Grüne Brücke.

Abb. 2. Semagramm in einem Lehrbuch der Kombinatorik („nieder mit dem sowjetimperialismus“)

Ein zweites steganographisches Prinzip besteht im Punktieren ausgewählter Zeichen in einem Buch oder in einer Zeitung. Es fällt sehr viel mehr auf als das obige Vorgehen (wenn es nicht mit einer Geheimtinte geschieht), ist aber einfacher zu bewerkstelligen. Eine Variante (in einem bekannten Buch über Kombinatorik) benutzt kaum merklich tiefgestellte Buchstaben (Abb. 2).

Arnold dear, it was good news to hear that
you have found a job in Paris. Anna hopes
you will soon be able to send for her. She's
very eager to join you now the children are
both well. Sonia

Abb. 3. Sichtbare Tarnung eines numerischen Codes mittels Absetzen im Schriftzug

Ein drittes Prinzip verwendet bei Handschriften das Absetzen im Wort als Kennzeichnung (Abb. 3). Im Beispiel ist allerdings nicht der Buchstabe gemeint, der vor oder nach der Unterbrechung steht, sondern es wird gezählt, nach wievielen Buchstaben ein Buchstabe mit einem nach oben gerichteten Abschwung steht – also 3 3 5 1 5 1 4 1 2 3 4 3 3 3 5 1 4 5 ..... (mehr darüber s. ‚Anarchistenchiffre‘, 3.3). Dieses steganographische Prinzip wurde in Frankreich 1895 von *A. Boetzel* und *Charles O'Keenan* den Autoritäten vorgeführt (die sich nicht zu Unrecht ablehnend verhielten), ebenfalls

in Verbindung mit einem numerischen Code. Es scheint jedoch in russischen Anarchistenkreisen bereits bekannt gewesen zu sein, und zwar eben im Zusammenhang mit der oben erwähnten Anarchistenchiffre. Es wurde auch von gefangenen deutschen U-Boot-Offizieren verwendet, die über alliierte U-Boot-Bekämpfungstaktik nach Hause berichteten.

In all diesen Fällen handelt es sich bei den Semagrammen um ‚sichtlich getarnte Geheimschriften' (*Hüttenhain*). Und es gibt viele mehr: Seit der Antike bekannt ist das Astragal des *Æneas*, bei dem durch Löcher geschlungenes Garn Buchstaben symbolisiert. Eine Schachtel voll Dominosteine mag ebenso eine Nachricht verbergen (durch die Stellung der Steine) wie eine Sendung von Taschenuhren (durch die Stellung der Zeiger). Die tanzenden Männchen von *Sherlock Holmes* (Abb. 4) tragen ebenso Nachricht wie ein versteckter Morsecode (Abb. 5): "*Compliments of CPSA MA to our chief Col. Harold R. Shaw on his visit to San Antonio May 11*th *1945*". *Shaw* war seit 1943 Chef der Zensurbehörde (*Technical Operations Division*) der US-Regierung.



Abb. 4. Von *Sherlock Holmes* gelöste Geheimnachricht (AM HERE ABE SLANEY), aus "Adventure of the Dancing Men" von *Arthur Conan Doyle*

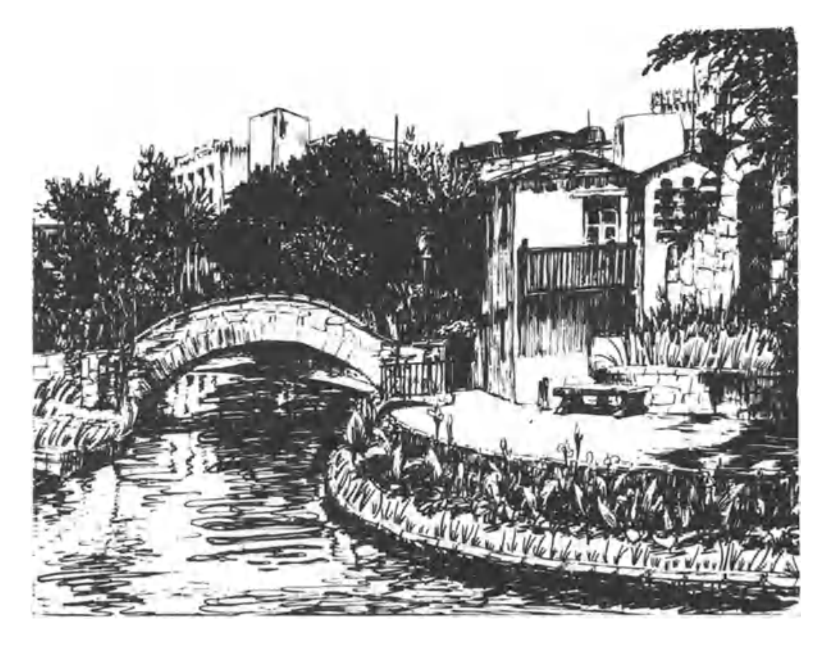


Abb. 5. Semagramm. Die Nachricht steht im Morsecode, der aus kurzen und langen Grashalmen links von der Brücke, entlang des Flusses und auf der kleinen Mauer gebildet wird

Labyrinth: Wo wird der Ballon niedergehen, A or B?

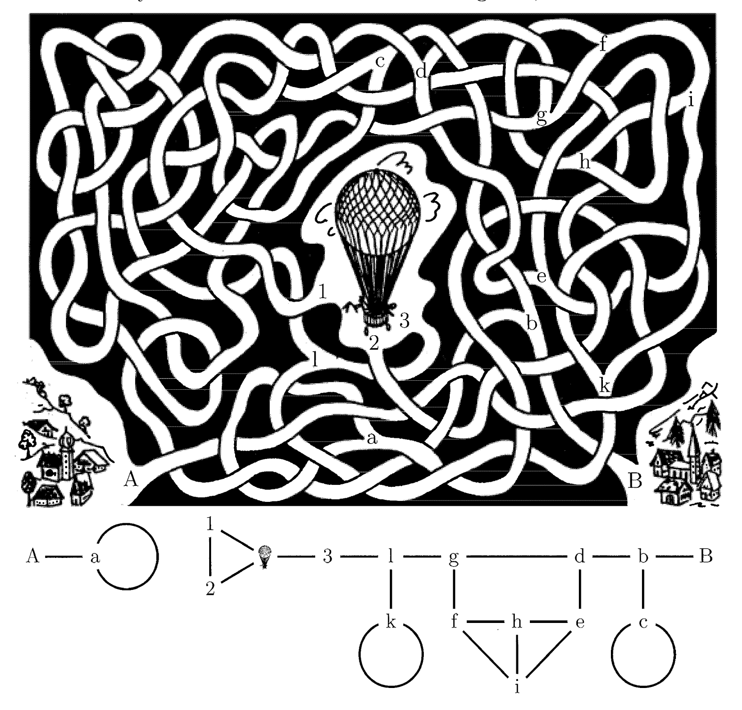


Abb. 6. Labyrinth und zugehöriger Graph

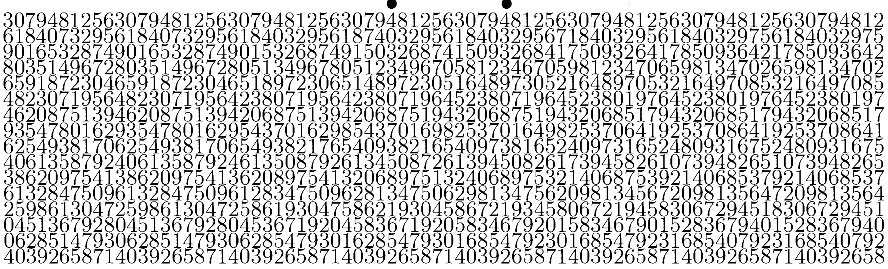


Fig. 7. Autostereogramm

Wie man klar Ersichtliches hinter einem Wust von unwesentlichen Details verbirgt, zeigen schlagend die Labyrinthe: Die verschlungenen Wege von Abb. 6 reduzieren sich auf einen Graphen, den man ‚auf den ersten Blick' versteht. Auch Autostereogramme, wie sie vor einiger Zeit in Mode gekommen sind, eignen sich vorzüglich zum Verstecken von Bildern (Abb. 7)

Von eigentlichem Interesse sind jedoch, wie gesagt, solche Verfahren der linguistischen Steganographie, die durch Gebrauch von ‚unersichtlich getarnten Geheimschriften' (nach *Hüttenhain/OKW*) eine geheime Nachricht als unverfänglich und offen (anders) verständlich ausgeben (engl. *open code*). Sie stehen methodisch der Kryptographie näher. Dabei gibt es wiederum zwei Klassen: *Maskierung* (mit der Unterklasse der *Stichwörter*) und *Verschleierung*.

1.3 Maskierung

Eine als offene Nachricht **maskierte Geheimschrift** (engl. *masked secret writing*) erfordert vorherige Absprache über die wahre Bedeutung unverfänglicher Floskeln. Hierin dürfte die älteste Form von Geheimhaltungstechniken liegen – sie findet sich in allen Kulturen. Orientalischen und fernöstlichen, aber auch manchen westlichen Händlern und Spielern wird Meisterschaft im Gebrauch von maskierenden Gesten und Ausdrücken nachgesagt. Unter amerikanischen Kartenschwindlern soll folgendes System bekannt sein: Die Art, die Zigarette zu halten und sich zu kratzen, zeigt Farbe oder Hände an. Eine Hand vor die Brust gehalten, mit abgestrecktem Daumen, bedeutet "*I am going to take this game. Anybody want to partner with me?*" Eine rechte Hand, Handfläche nach unten, auf dem Tisch bedeutet "*Yes*" , eine Faust "*No, I'm working single, and I discovered this guy first, so scram*" .

Der französische Zauberkünstler *Robert Houdin* (1805–1871) soll um 1845 ein ähnliches System benutzt haben, mit I , M , S , V für *cœur*, *carreau*, *trèfle*, *pique*; ≪*il fait chaud*≫ oder ≪*il y a du monde*≫ bedeutet I = „ich habe Herz". In englischen Whist-Clubs der viktorianischen Zeit ging es nicht viel besser zu, "Have you seen old Jones in the past fortnight" würde Herz bedeuten, da es mit /H/ beginnt. Auf der Bridge-Weltmeisterschaft in Buenos Aires 1965 geriet das britische Team in den Verdacht, Signale ausgetauscht zu haben – natürlich konnte nichts bewiesen werden.

Manchmal wird eine geheime Nachricht in unverfänglicher Weise maskiert unter Ausnutzung von Umständen, die nur dem Sender und dem Empfänger bekannt sind. Das kann auch im Alltag vorkommen. Ein berühmtes Beispiel hat Katja Mann berichtet: Sie telefonierte im März 1933 aus Arosa in der Schweiz mit ihrer Tochter Erika in München und sagte: „Ich weiß nicht, es muß doch jetzt bei uns gestöbert werden, es ist doch jetzt die Zeit." Aber Erika erwiderte „Nein, nein, außerdem ist das Wetter so abscheulich. Bleibt ruhig noch ein bissel dort, ihr versäumt ja nichts". Nach diesem Gespräch war es Thomas und Katja Mann klar, daß sie nicht nach Deutschland zurückkehren konnten, ohne sich in Gefahr zu begeben.

Von den Vaganten des Mittelalters bis zu den Pennern, Tramps und Tippelbrüdern (den ‚Kunden') findet man den Gebrauch von Geheimzeichen. Abb. 8 zeigt einige ‚Zinken', wie man sie in den dreißiger Jahren in einer mitteleuropäischen Kleinstadt noch finden konnte: die Warnung vor der Wohnung eines Polizisten und vor einem gewalttätigen Hausbesitzer, Abb. 9 ein Gegenstück aus dem amerikanischen Mittelwesten.



Abb. 8. ‚Zinken', die vor der Wohnung eines Polizisten und vor einem gewalttätigen Hausbesitzer warnen

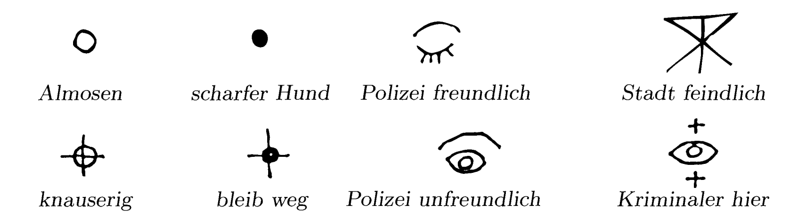


Abb. 9. Geheimzeichen für „Polizei freundlich" und „Polizei unfreundlich" und andere Botschaften (Mittelwesten der Vereinigten Staaten, erste Hälfte 20. Jh.)

Winzige Geheimzeichen werden auch in Gravüren für Briefmarken oder Banknoten als Merkmal für den Graveur oder Drucker verwendet.

Sondersprachen beruflicher und gesellschaftlicher Art, allgemein **Jargon** genannt, vor allem aber ihre Spielarten aus dem Milieu der Bettler, Vagabunden und Gauner: Argot (Frankreich), Alemania (Spanien), Cant (England), Thieves' Latin (England), Rotwelsch (Deutschland), Fourbesque (Italien), Calão (Portugal), die der Abschirmung (und dem Zusammenhalt) einer sozialen Gruppe geradezu dienen, bedienen sich oft der Maskierung. Maskierte Geheimschriften oder -sprachen heißen deshalb auch englisch *jargon codes*.

Der älteste päpstliche Code im 14. Jahrhundert benutzte ‚Ägypten' für Ghibellinen, ‚Söhne Israels' für Guelfen. Ein französischer Code des 17. Jahrhunderts benutzte ausschließlich Jargon: *Jardin* für Rom, *La Roze* für den Papst, *Le prunier* für den Cardinal de Retz, *La fenestre* für den Bruder des Königs, *L'écurie* (‚Ritterschaft') für Deutschland, *Le roussin* für den Herzog von Bayern und so weiter.[4]

Steganographisch besonders interessant sind die Sprachen der kriminellen Zirkel. Der französische Argot bietet genügend Beispiele. In die Umgangssprache eingedrungen sind *rossignol* (Nachtigall) für Nachschlüssel (‚Dietrich'), nachgewiesen seit 1406; *mouche* (Fliege) für Spion (‚Spitzel'), bekannt seit 1389. Häufig benutzt man sprachlichen Anklang: *rebecca* für *rebellion*, *limace* (Nacktschnecke) für *lime* (Feile) – welch letzteres Fourbesque ist für Hemd; *marquise* für *marque* (Mal, Narbe) – was Alemania ist für Mädchen; oder *frisé* (Lockiger) für *fritz* (populär für Deutscher). Nicht so unverfänglich sind die **Metaphern**: *château* (Schloß) für *hôpital*, *mitraille* (Kugel) für *petite monnaie* (Kleingeld), oder gar die berüchtigten Metaphern *marmite* (Kochtopf) für die erste Frau des Zuhälters, *sac à charbon* für den Priester. Auch sarkastische Metaphern wie *mouthpiece* für Rechtsanwalt kommen vor.

Wahrhaft international sind ‚Loch' – *trou* für Gefängnis, ‚Schnee' – *neige* – *snow* für Kokain, dito *sucre* – *sugar* ; ‚heiß' – *hot* für kürzlich gestohlene Ware, ‚abstauben' – *nettoyer* für stehlen, ‚Kies' – *galette* (frz. *galet*, der Kieselstein) – *rock* für Geld. Alle Arten von Wortspielen und Kalauern gehören prinzipiell hierher. Das britische 'Twenty Committee' aus dem

[4] Auch bei einer bonapartistischen Verschwörung 1831 wurde noch eine simple Maskierung zeitgeschichtlicher Namen verwendet.

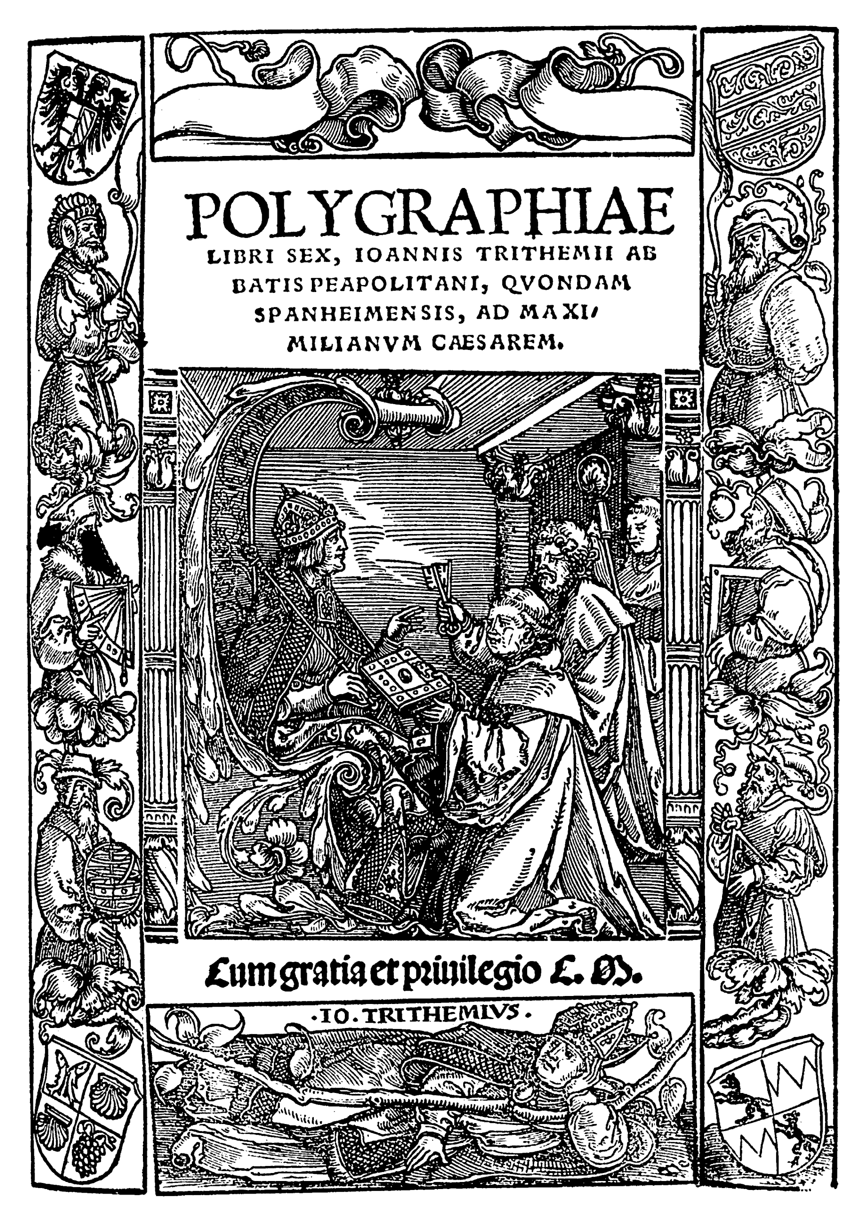


Abb. 10. Titelseite (Holzschnitt) des ersten gedruckten Werkes über Kryptographie (1518)

2. Weltkrieg, das auf Doppelagenten spezialisiert war, war nach der römisch geschriebenen Zahl XX benannt, wobei XX für 'Double Cross' steht.

Gut maskierte Geheimschriften für einigermaßen *universellen* Gebrauch sind schwierig zu entwickeln und noch schwieriger richtig zu gebrauchen — der geübte Zensor merkt leicht das ‚Gestelzte' fabrizierter Sprache.

Trithemius gab in seiner *Polygraphiae* von 1508 — gedruckt nach seinem Tode (1518) (Abb. 10) — eine Sammlung lateinischer Wörter als Codewörter

für Einzelbuchstaben (Abb. 11), den *Ave Maria Code*. So konnte "*abbé*" als "DEUS CLEMENTISSIMUS CREATOR MAGNUS" maskiert werden. Vielleicht würden heutige Zensoren nicht mehr so viel Latein können, um damit fertig zu werden.

A	Deus	A	clemens
B	Creator	B	clementiſsimus
C	Conditor	C	pius
D	Opifex	D	pijſsimus
E	Dominus	E	magnus
F	Dominator	F	excelſus
G	Conſolator	G	maximus
H	Arbiter	H	optimus

Abb. 11. Anfang von *Trithemius' Ave Maria Code*

Eine beliebte Sicherheitsmaßnahme der Zensoren ist es, Nachrichten semantisch korrekt umzuformulieren. Im 1. Weltkrieg änderte ein Zensor eine Depesche "*Father is dead*" in "*Father is deceased*". Zurück kam über die Leitung die Nachricht "*Is father dead or deceased?*".

Auch **allegorische Sprache** hilft nur wenig. In der Diplomatie *Ludwigs* XV. gab man 1755 dem *Chevalier Douglas* für eine geheime Mission nach Rußland ein allegorisches Arsenal aus der Pelzhändlerbranche mit: ≪*Le renard noir était cher*≫ „der Einfluß der englischen Partei steigt"; ≪*L'hermine était en vogue*≫ „der Einfluß der russischen Partei steigt"; ≪*Le loup-cervier avait son prix*≫ „die österreichische Partei (unter *Bestuscheff*) behielt ihren überwiegenden Einfluß". Der preussenfreundliche *Bestuscheff* war ≪*Le loup-cervier*≫ und ≪*Un peau de petit-gris*≫ waren 3 000 Söldner in englischen Diensten.

Hoffentlich war der *Chevalier Douglas* in der Verwendung seines allegorischen Codes geschickter als die deutschen Spione, die im 1. Weltkrieg in der Rolle holländischer Kaufleute Zigarren in Größenordnungen von 10 000 Stück an einem Tag aus Portsmouth, am nächsten Tag eine große Menge aus Plymouth und aus Devonport, später 5 000 Stück aus Newcastle und so weiter bestellten – 1 000 Coronas bedeuteten einen Kreuzer. Ihr unzureichendes System brachte ihrem Leben am 30. Juli 1915 ein vorzeitiges Ende.

Besser erging es *Velvalee Dickinson*, einer japanophilen Dame in New York City, die 1944 einen regen Postverkehr über zerbrochene und reparaturbedürftige Puppen unterhielt. Sie wurde entdeckt, als ein unter falschem Absender gesandter Brief an eine Adresse in Portland, Oregon, zurückkam. Die Dame unterhielt tatsächlich einen exquisiten Puppenladen in New Yorks Madison Avenue. Technical Operations Division (die U.S. Zensurbehörde) und das FBI überführten sie, aber sie kam mit 10 Jahren Gefängnis und $ 10 000 Strafe davon.

Und in dem Audrey-Hepburn-Film “Breakfast at Tiffany’s” wandert Miss Holly Golightly für eine Nacht hinter Gitter, weil sie einem Gangster hilft, mittels ‚Wetternachrichten‘ seinen Kokainhandel vom Gefängnis aus zu betreiben – ihr fiel lediglich auf, daß *“snow in New Orleans”* recht unwahrscheinlich klang.

Tag / Uhrzeit / Ort und Art der Unterkunft	Darstellung der Ereignisse (Dabei wichtig: Beurteilung der Lage [Feind- und eigene], Eingangs- und Abgangszeiten von Meldungen und Befehlen)
5.6.44	Am 1., 2. und 3.6.44 ist durch die Nast innerhalb der
	"Messages personelles" der französischen Sendungen des
	britischen Rundfunks folgende Meldung abgehört worden :
	"Les sanglots longs des violons de l'autómme ".
	Nach vorhandenen Unterlagen soll dieser Spruch am 1. oder
	15. eines Monats durchgegeben werden, nur die erste Hälfte
	eines ganzen Spruches darstellen und ankündigen, dass
	binnen 48 Stunden nach Durchgabe der zweiten Hälfte des
	Spruches, gerechnet von 00.00 Uhr des auf die Durchsage
	folgenden Tages ab, die anglo-amerikanische Invasion be-
	ginnt.
21.15 Uhr	Zweite Hälfte des Spruches "Blessent mon coeur d'une longeur
	monotone" wird durch Nast abgehört.
21.20 Uhr	Spruch an Ic-AO durchgegeben. Danach mit Invasionsbeginn
	ab 6.6. 00.00 Uhr innerhalb 48 Stunden zu rechnen.
	Überprüfung der Meldung durch Rückfrage beim Militärbe-
	fehlshaber Belgien/Nordfrankreich in Brüssel (Major von
	Wangenheim).
22.00 Uhr	Meldung an O.B. und Chef des Generalstabes.
22.15 Uhr	Weitergabe gemäss Fernschreiben (Anlage 1) an General-
	kommandos. Mündliche Weitergabe an 16. Flak-Division.

Abb. 12. Ausschnitt aus einem Tagebuch der Funkaufklärung der 15. Armee (Oberstleutnant *Meyer*, Feldwebel *Reichling*). *automme* ist als *automne* zu lesen, *longeur* als *langueur*.

1.4 Stichwörter

Der wichtigste Spezialfall einer Maskierung betrifft die Verwendung eines **Stichwortes** (frz. *mot convenu*, engl. *cue*) oder eines Satzes, Verses mit einer einzigen, vorherbestimmten Bedeutung. Die Wichtigkeit der Nachricht ist hier an den Zeitpunkt der Aussendung gebunden, die Nachricht ist ein **Alarm** oder eine **Quittung**. Eine große Anzahl von Nachrichten wurde durch die BBC an die *résistance* in Westeuropa ausgesandt. Damit fielen auch einige maskierte Nachrichten, die an verborgener Wichtigkeit die anderen um Größenordnungen überragten, nicht sonderlich auf, so etwa am 1. Juni 1944 in den 21-Uhr-Nachrichten von BBC einige *personal messages*,

darunter von der ersten Strophe des Gedichts *Chanson d'Automne* von *Verlaine* (wörtlich: „Die langen Schluchzer der Violinen des Herbstes verwunden mein Herz mit eintönigem Schmachten") die erste Hälfte. Am 5. Juni 1944 kam die zweite Hälfte. *Canaris'* Abwehr hatte schon im Januar 1944 die Kommandeure der Westfront über den *jargon code* und seine Bedeutung informiert (Abb. 12). Als die 15. Armee das erwartete Stichwort auffing, wurden alle deutschen Kommandostellen alarmiert – aus bis heute unerklärlichen Gründen erreichte der Alarm jedoch die deutsche 7. Armee, in deren Küstenbereich die Invasion am 6. Juni 1944 stattfand, nicht.

Auch die Japaner hatten das System 1941 benutzt. Zum Beispiel sollte HIGASHI NO KAZE AME („Ostwind, Regen"), in den Wetterbericht der Überseenachrichten eingeschoben und zweimal wiederholt, ‚Krieg mit U.S.A.' ankündigen. Die U.S. Navy fing am 19. November einen diesbezüglichen diplomatischen Funkspruch ab und konnte ihn bis zum 28. November 1941 entziffern. Als die Spannung wuchs, überwachten zahlreiche Funkaufklärungsstationen der U.S.A. den japanischen Radioverkehr auf das Stichwort hin. Es kam am 7. Dezember 1941 – Stunden nach dem Angriff auf Pearl Harbour – in der Form NISHI NO KAZE HARE („Westwind, klar"), und kündigte, was niemand mehr überraschte, den Ausbruch der Feindseligkeiten mit Großbritannien an. Vielleicht handelte es sich um einen ‚Doppelpflanz' der Japaner.

Bei professioneller Verwendung stehen die maskierten Geheimschriften den chiffrierten nahe (s. 2.2); sie zeigen eine Verwandtschaft zu Codierungen (4.4).

1.5 Verschleierung: Würfel

Von anderer Natur als die maskierten Geheimschriften sind die als offene Nachricht **verschleierten** Geheimschriften (engl. *concealment cipher*). Hier ist die zu übermittelnde Nachricht eingebettet in die zu übermittelnde, unverfängliche offene Nachricht, was durch Hinzufügen von **Blendern**, **Nieten**, **Füllzeichen**, **Nullen** (frz. *nonvaleurs*, engl. *nulls*, *dummies*) erreicht wird.

Um die eigentliche Nachricht wiederzufinden, muß der Platz, an dem sie steht, verabredet sein. Dazu bieten sich zwei Möglichkeiten für *garbage-in-between* an: Regeln anzugeben (‚Würfel', engl. *null cipher, open-letter cipher*) oder Raster (frz. *grille*, engl. *grille*) zu verwenden.

Regeln für verschleierte Geheimschriften sind häufig von der Art „das x-te Zeichen nach einem bestimmten Zeichen", z.B. „das erste Zeichen nach Zwischenraum" (engl. *family code*, im 2. Weltkrieg von Soldaten gern gebraucht, zum großen Mißvergnügen des Zensors), besser schon „das dritte Zeichen nach Zwischenraum" oder „das dritte Zeichen nach Interpunktionszeichen". Solche verschleierte Geheimschriften nennt man engl. *acrostics*. Ein geübter Zensor erkennt diese Tarnung meist sogleich an der ‚gestelzten' Sprache, und sein scharfes Auge erfaßt sicher, was sich hinter

P̆RESIDENT'S ĔMBARGO R̆ULING S̆HOULD H̆AVE
ĬMMEDIATE N̆OTICE. ĞRAVE S̆ITUATION ĂFFECTING
ĬNTERNATIONAL L̆AW. S̆TATEMENT F̆ORESHADOWS
R̆UIN ŎF M̆ANY N̆EUTRALS. Y̆ELLOW J̆OURNALS
ŬNIFYING N̆ATIONAL ĔXCITEMENT ĬMMENSELY

verbirgt – eine im 1. Weltkrieg abgefangene Nachricht. Wenn nötig, hilft es, eine Nachricht wortweise auszurichten:

    ↓
I N S P E C T
D E T A I L S
F O R
T R I G L E T H
A C K N O W L E D G E
T H E
B O N D S
F R O M
F E W E L L

Die Tarnung fällt dann ab, der ,Klartext' *springt ins Auge*.

Seine gute Vorstellungskraft rettete *Sir John Trevanion*, der zu *Oliver Cromwells* Zeiten lebte, das Leben: Er fand im Brief seines Freundes *R.T.* die Botschaft *"Panel at east end of chapel slides"* (Abb. 13) und fand auch die Tür.

> Worthie Sir John:— Hop̆e, thăt is ye beste comfort of ye afflicted, can̆not much, I fĕar me , hel̆p you now. Thăt I would saye to you, is t̆his only: if ĕver I may be able to requite that I do owe you, stănd not upon asking me. 'Tis̆ not much that I can do: but̆ what I can do, beĕ ye verie sure I wille. I kn̆owe that, if d̆ethe comes, if ŏrdinary men fear it, it f̆rights not you, accŏunting it for a high honour, to h̆ave such a rewarde of your loyalty. Prăy yet that you may be spared this soe bitter, cup̆. I fĕar not that you will grudge any sufferings; onl̆y if bie submission you can turn them away, 'tis̆ the part of a wise man. Tel̆l me, an ĭf you can, to d̆o for you anythinge that you wolde have done. Thĕ general goes back on Wednesday. Res̆tinge your servant to command. — R. T.

Abb. 13. Nachricht an *Sir John Trevanion: Panel at east end of chapel* slides (dritter Buchstabe nach Interpunktionszeichen)

Es wird von einem Soldaten *Eisenhowers* berichtet, der 1942 seinen Eltern den Ort, in dem er sich aufhielt, durch den jeweils ersten Buchstaben (nach der Anrede) in seinen Briefen mitteilen wollte – kryptographisch und steganographisch zunächst kein schlechter Einfall. Die Sache kam trotzdem heraus, als die Eltern schrieben: „Wo ist Nutsi – wir finden es in unserem Atlas nicht?" Der Ärmste hatte vergessen, seine Briefe mit dem Datum zu versehen.

Als **Akrostichon** hat diese Technik sogar in die schöngeistige Literatur Eingang gefunden. Beim klassischen Akrostichon waren die Anfangsbuchstaben, -silben oder -wörter aufeinanderfolgender Verse, Strophen, Abschnitte oder Kapitel von Bedeutung. Man chiffrierte so Wörter, Namen oder Sätze (Abb. 14), häufig mit Bezug auf den Autor. Das Akrostichon diente auch als Schutz gegen Auslassungen und Einfügungen; ein früher Fall einer fehlersichernden Codierung. Ähnlich wird beim **Chronogramm** in einer Inschrift eine (römisch geschriebene) Zahl verborgen, meist eine Jahreszahl, zum Beispiel der Anbringung der Inschrift:

In der Kirche des ehemaligen Zisterzienser-Klosters Fürstenfeld an der Amper wurde 1766 eine Statue des Stifters Ludwig der Strenge (1229–1294) aufgestellt, darunter findet sich auf einer Tafel das Chronogramm

LVDoVICVs seVerVs DVX baVarVs aC paLatInVs,
hIC In sanCta paCe qVIesCIt.

(Ludwig der Strenge, Herzog von Baiern und der Pfalz, ruht hier in heiligem Frieden.)

Besteht das Chronogramm aus einem Vers oder aus zwei Versen, heißt es **Chronostichon** oder **Chronodistichon**.

LITERATUR

Schnellschreibmethode

Er soll, so berichtet Robert K. Merton, bei all dem, was er schrieb, eine besondere Technik entwickelt haben, die so einfach gewesen sein muß, daß es seine Kollegen und Neider das Staunen lehrte, weil bereits wenige Wochen nachdem seine erste Abhandlung veröffentlicht war, die nächste folgte, kein Wort und keine Seite dünner und von ebensolcher Prägnanz, daß jeder andere Monate, wenn nicht Jahre dazu gebraucht hätte, um Zeile für Zeile zu füllen. Sein Geheimnis soll Thomas Fuller auf Drängen seiner Freunde aber in kleinster abendlicher Runde ein oder zwei Tage vor seinem Tod zugegeben haben auf einem Blatt, auf dem er in einer bestimmten Weise Worte anordnete und das er ihnen vorlegte mit der süffisanten Bemerkung, er füllte ihnen lieber noch einmal ihre Gläser vor der Lösung, hernach würde ihnen keine Ruhe mehr bleiben, bis auch sie den Versuch selbst unternommen hätten, die Methode, die im übrigen in der Poesie schon seit langem einen breiten Raum einnehme, auch auf ihre Wissenschaft anzuwenden, um so aus schönen Worten exakte Aussagen entstehen zu lassen.

LUDGER FISCHER

Abb. 14. Akrostichon aus SZ Magazin, 28.3.1991

Komponisten haben Nachrichten verborgen in den Noten, entweder (Beispiel B A C H) direkt hinter den Tonbezeichnungen einer melodischen Floskel oder mit Hilfe eines Zahlenalphabets: Kommt der i-te Ton der Tonleiter k mal vor, ist an i-ter Stelle der k-te Buchstabe des Alphabets hinzuschreiben.

J. S. Bach bediente sich auch gern dieser Chiffre; so kommt im Orgelchoral ‚Vor deinen Thron', 1750, in der viertaktigen Melodiefloskel, die in G-Dur steht, g zweimal (B), a einmal (A), h dreimal (C) und c achtmal (H) vor.

Blender werden auch in manchen Jargons verwendet: Bloßes Anhängen einer Silbe als Blender (**parasitäre Suffixation**) ist das einfachste und älteste System, im Französischen

FLOUTIERE	für *flou* , Argot für	‚weg!'
GIROLLE	für *gis* , Argot für	‚ja'
MEZIS	für *me* ,	
ICICAILLE	für *ici*	

mit hunderten ähnlicher Bildungen. Schon bei *Cartouche* (18. Jh.) findet sich **Vous**ierge **trouv**aille **bon**orgue **ce gigot**mouche.

Tut Latin, eine Schülersprache im Englischen, setzt TUT zwischen alle Silben. Solche Schülerjargons scheinen sehr alt zu sein, schon 1670 wird aus Metz (Lothringen) von einem ‚Stotterer-System' berichtet, wo etwa *undreque foudreque* für *un fou* steht. Hierher gehört auch das **Javanais**:

LAVEBLAVANC	steht für *le blanc*
NAVON	steht für *non*
JAVE	steht für *je* (Argot für ‚ja')
CHAVAUSSAVURAVE	steht für *chaussure* .

Andere Systeme verwenden Blender mit Vokalwiederholung, etwa im Deutschen die B-Sprache:

GABARTEBENLAUBAUBEBE steht für gartenlaube

und im Französischen das **Cadogan**:

CADGADODGOGADGAN steht für *cadogan.*

Joachim Ringelnatz [*Hans Bötticher*] verfaßte ein Gedicht in der Bi-Sprache (Abb. 15).

Gedicht in Bi-Sprache

Ibich habibebi dibich,
Lobittebi, sobi liebib.
Habist aubich dubi mibich
Liebib? Neibin, vebirgibib.

Nabih obidebir febirn,
Gobitt seibi dibir gubit.
Meibin Hebirz habit gebirn
Abin dibir gebirubiht.

Abb. 15. Gedicht in Bi-Sprache von *Joachim Ringelnatz*

Kompliziertere Systeme arbeiten zusätzlich mit einer Buchstabenumstellung[5] (Transposition, s. 6.1). Aus dem Milieu stammt das **Largonji**:

LEUDÉ	für	*deux francs*
LINVÉ	für	*vingt sous*
LARAQUÉ	für	*quarante sous*

mit den phonetischen Abarten

LINSPRÉ	für	*prince* (*Vidocq* 1837)
LORCEFÉE	für	*La Force*, ein Pariser Gefängnis .

und das **Largonjem**:

LONBEM	für	*bon* (1821)
LOUCHERBEM	für	*boucher*
OLRAPEM	für	*opéra* (1883) .

Das Wort Largonji ist auf diese Weise aus Jargon gebildet. Eine Variante mit Unterdrückung des Anfangskonsonanten zeigt das **Largondu**:

LAVEDU	für	*cave*
LOQUEDU	für	*toque*
LIGODU	für	*gigo(t)* .

Anderen, ähnlichen Bildungsgesetzen folgen

LOCROMUCHE	für	*maquerau*
LEAUBICHE	für	*beau*
NEBDUTAC	für	*tabac* (1866)
LICELARGU	für	*cigare* (1915) .

Diese Systeme haben Parallelen in Ostasien.

Pig Latin, eine andere Schülersprache, setzt AY ans Ende eines zyklisch permutierten Wortes: third wird IRDTHAY. Cockneys haben eine Reimsprache mit Blendern: TWIST AND TWIRL für *girl*, JAR OF JAM für *tram*, STORM AND STRIFE für *wife*, BOWL OF CHALK für *talk*, FLEAS AND ANTS für *pants*, APPLES AND PEARS für *stairs*, BULL AND COW für *row*, CAIN AND ABEL für *table*, FRANCE AND SPAIN für *rain*, PLATES OF MEAT für *feet*, LOAF OF BREAD für *head*. Das eigentliche Reimwort wird dabei häufig auch weggelassen – der Eingeweihte denkt es sich, und LOAF oder PLATES beispielsweise wurden so zu umgangssprachlichen Ausdrücken, deren Herkunft den meisten heute unbekannt ist (**Lexikalisierung**).

Wenig Mühe gab sich *Jonathan Swift* (1667–1745) in seinem *Journal to Stella*, die in Wirklichkeit *Esther Johnson* (1681–1728) war: In einem kompromittierenden Brief vom 24. Febr. 1711 bestand seine Vorsicht lediglich darin, daß jedes zweite Zeichen ein Blender war.

[5] Reines Rückwärtslesen (‚Krebs') kommt im Cant ebenfalls vor: OCCABOT für *tobacco*; KOOL für *look*; YOB („Lümmel") für *boy*; SLOP für *police*. Reine Silbenumstellung gibt es im *Verlan* (von *l'envers*): NIBERQUE für *bernique* (‚nichts da', ‚weit gefehlt') von frz. *berniches*, kleine Muscheln; LONTOU für *Toulon*; LIBRECA für *calibre*, Schießeisen; DREAUPER („Polizist") für *perdreau*, Rebhuhn; RIPOU für *pourri*, verfault; BEUR für *rebeu* (arabisch).

1.6 Verschleierung: Raster

Die auf *Geronimo Cardano* (in *De Subtilitate, 1550*) zurückgehende Methode, **Raster** (frz. *grille*, engl. *grille*) zu verwenden, ist simpel, aber unbequem. Sie hat auch den Nachteil, daß beide Seiten den Raster besitzen und bewahren müssen — bei einem Soldaten oder Gefangenen keine Selbstverständlichkeit. Hätte *Lord Byron* (1788–1824), der allerdings kein gewöhnlicher Soldat war, diese Methode benutzt, so wären ihm seine poetischen Fähigkeiten sehr zustatten gekommen, um ein Gedicht abzufassen wie das von Abb. 16; vermutlich besaß er auch das Talent, das ganze so hübsch zu schreiben, daß der Klartext zwanglos in die Rasterfenster paßte.

And there was mounting in hot haste the steed,
The mustering squadron and the clattering car,
And swiftly forming in the ranks of war;
And deep the thunder peal on peal afar;
And near, the beat of the alarming drum
Roused up the soldier ere the morning star
While thronged the citizens with terror dumb
Or whispering, with white lips, — 'the
foe! they come, they come!'

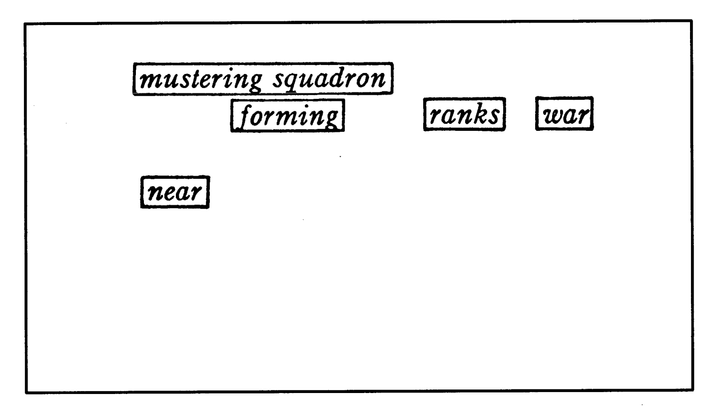


Abb. 16. *Lord Byrons* hypothetische Nachricht

Cardano forderte übrigens, die so gewonnene Nachricht dreimal abzuschreiben, um jede Schreibunregelmäßigkeit zu verwischen. Die Methode wurde im 16. und 17. Jahrhundert im diplomatischen Verkehr gelegentlich benutzt. Kardinal *Richelieu* soll sich ihrer bedient haben.

Auch raffiniertere Regeln werden in der modernen Literatur erwähnt, etwa die Übermittlung von Dualzahlen (ihrerseits vermutlich gebraucht als Chiffrierung), wobei die Ziffer **O** durch ein Wort mit gerader Vokalanzahl, die Ziffer **L** durch ein Wort mit ungerader Vokalanzahl ausgedrückt wird.

Bei professioneller Verwendung stehen die verschleierten (unersichtlich getarnten) Geheimschriften meistens ebenfalls den chiffrierten Geheimschriften nahe (s. 2.2); sie zeigen eine gewisse Verwandtschaft insbesondere in der Verwendung von Blendern (s. 2.3.1) und der Transposition (s. 6.1).

1.7 Klassifizierung der kryptographischen Methoden

Eine graphische Übersicht über die in diesem Kapitel gewonnene Klassifizierung der kryptologischen Methoden zeigt Abb. 17.

Wir haben Maskierung und Verschleierung so ausführlich behandelt, weil sie uns methodisch leiten können: die Maskierung zur Substitution, die Verschleierung zur Transposition, damit zu den beiden Grundelementen der Kryptographie, die wir im nächsten Kapitel einführen werden.

Außerdem lehrt uns die Steganographie bereits eine Maxime: Sprache hat Eigengesetzlichkeit, und schwerer noch als es ist, diese (in der Kryptographie) zu unterdrücken, ist es, sie zu imitieren, wie es in der Steganographie geschieht. Die linguistische Steganographie wird deshalb von reinen Kryptographen mit vorsichtiger Distanz behandelt; sie abzuwehren, ist Sache der Zensur. Ihrem Wesen nach ist ihr Gebrauch durch Amateure bereits unschädlich gemacht, wenn er unterbunden oder aufgedeckt wird; eine tatsächliche Entzifferung ist dann für die Zensurbehörde oft unwichtig (abgesehen vom Erbringen des Schuldbeweises in einem anschließenden Gerichtsverfahren).

Der professionelle Gebrauch linguistischer Steganographie kann nur in Einzelfällen geboten sein – es sei denn, es handle sich um eine Überdeckung eines vorangehenden echt kryptographischen Verfahrens.

Steganographie und die eigentliche Kryptographie fallen unter den allgemeinen Begriff der Kryptologie. Der lateinische Ausdruck *cryptologia* wurde, wie auch der Ausdruck *cryptographia*, erstmals 1641 von dem englischen Bischof *John Wilkins* benutzt, mit der Bedeutung *Geheimsprache*. 1645 wurde von *James Howell* der engliche Ausdruck *cryptology* geprägt; er schrieb "*cryptology, or epistolizing in a clandestine way, is very ancient.*" Der Gebrauch der Wörter *cryptography*, *cryptographie, crittografia*, *Kryptographie* hat bis unlängst auch dann das Feld beherrscht, wenn die Kryptanalysis eingeschlossen war. *Claude Shannon* nannte noch 1945 seinen vertraulichen Bericht über die Sicherheit gegen unbefugte Entzifferung *A Mathematical Theory of Cryptography*. Als Buchtitel wurde *cryptologue* von dem Schweden *Yves Gyldén* 1932 verwendet und *cryptologist* von *William F. Friedman* 1961; in moderner Zeit taucht *cryptology*



Claude Shannon (∗ 1916)

1963 auf im Titel eines Artikels von *David Kahn*; es wurde intern u. a. von *William F. Friedman* und *Lambros D. Callimahos* schon in the 50er Jahren benutzt. Mit *Kahns The Codebreakers* von 1967 wurde der Terminus 'cryptology' fest etabliert mit der Bedeutung, sowohl 'cryptography' als auch 'cryptanalysis' zu umfassen; er ist heute allgemein akzeptiert.

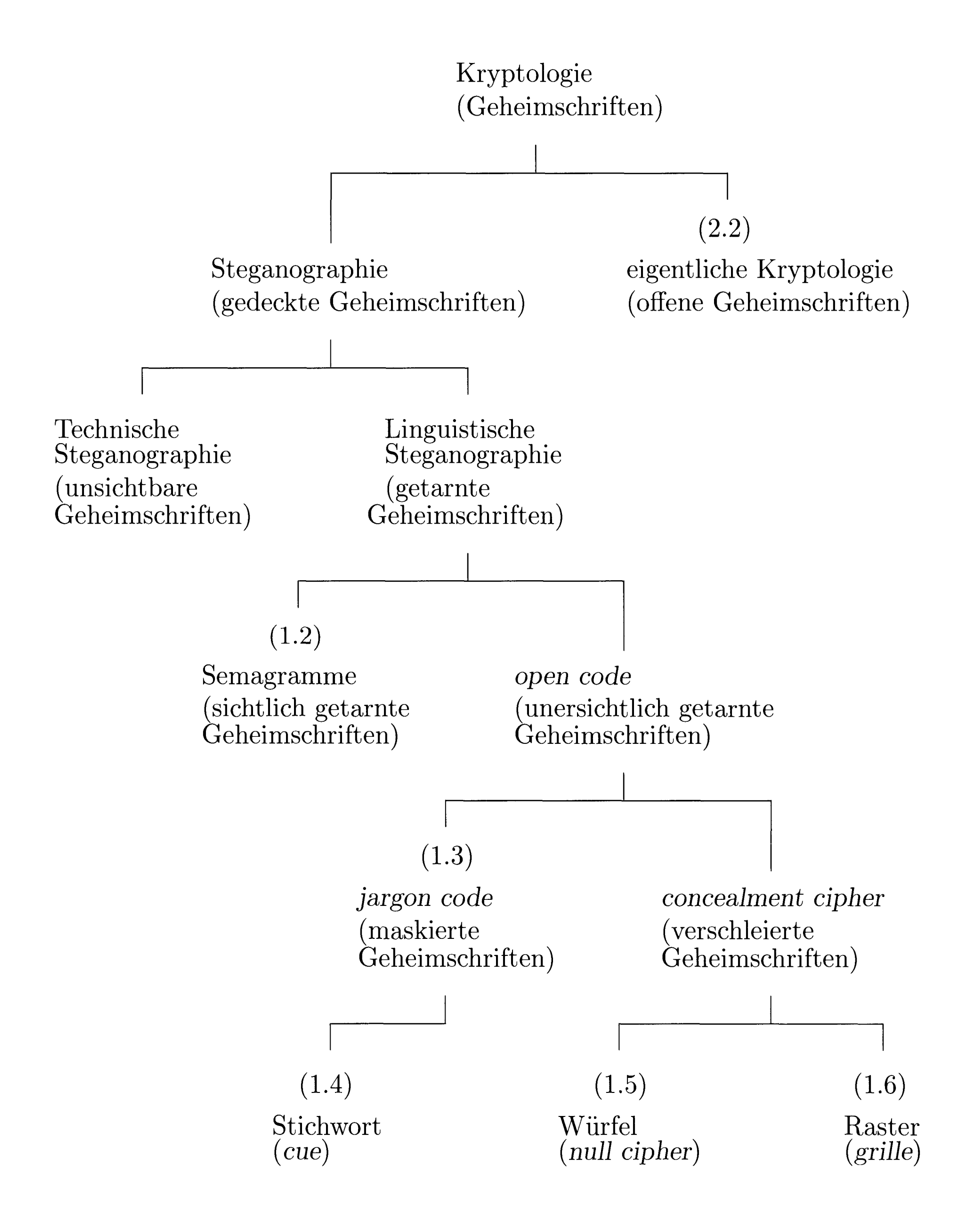


Abb. 17. Klassifizierung der kryptologischen Methoden

2 Aufgabe und Methode der Kryptographie

"Nearly every inventor of a cipher system
has been convinced of the unsolvability
of his brainchild."
Kahn

Der nachfolgend zu gebende Überblick über die bekannten kryptographischen Verfahren ist auf den Gesichtspunkt der Sicherung[1] von etablierten Nachrichtenwegen gegen (passives) unbefugtes Lauschen und Mitlesen (**Brechen**) sowie gegen (aktive) **Fälschung** abgestellt (ISO 7498). Die **Geheimhaltung** (engl. *secrecy*) zum Zwecke der Vertraulichkeit (engl. *confidentiality*) und der persönlichen Abgeschiedenheit (engl. *privacy*) ist das klassische Ziel. Die Sicherung gegen Fälschung und Unterschiebung, die **Authentisierung** (engl. *authentication*) ist erst neuerdings zu größerer Bedeutung gelangt.

Neben *mathematischen* spielen für die Kryptologie auch *philologische* Fragen eine große Rolle. Hierin besteht eine Verwandtschaft mit dem Gebiet der **Entzifferung verschollener Schriften und Sprachen**[2] (Farbtafel A), einem reizvollen Grenzgebiet der Archäologie und der Sprachwissenschaft.

2.1 Charakter der Kryptographie

Die klassische Aufgabe der Kryptographie ist es, eine Nachricht oder Aufzeichnung für den Unbefugten unverständlich zu machen. Eine solche Absicht kann leicht übertrieben werden – das macht die Nachricht dann auch für den berufenen Empfänger unleserlich. Wem ist es nicht schon passiert, daß er eine eilig niedergeschriebene Notiz nach Wochen oder schon nach Tagen nicht mehr lesen konnte.

Es ist fatal, wenn ein Fehler in der Chiffrierung gemacht wird oder auch, wenn – hauptsächlich im Funkverkehr durch atmosphärische Störungen – die Nachricht **verstümmelt** (engl. *garbled*) oder **sinnentstellt** (engl. *corrupted*) wird. Der dann naheliegende Versuch, die gleiche Nachricht noch

---

[1] Bloßen Störungen des Nachrichtenweges durch physikalisch-technische Effekte wird seit den Entdeckungen von *Shannon* und *Hamming* um 1950 durch fehleranzeigende und -korrigierende Codierungen begegnet, die hier nicht behandelt zu werden brauchen.

[2] *J. Friedrich*, Entzifferung verschollener Schriften und Sprachen, Springer, Berlin 1954.

einmal – und diesmal richtig – zu chiffrieren und zu übertragen, ist ein schweres Sicherheitsrisiko (11. Kapitel, Chiffrierfehler). Dazu *W. Kozaczuk*: *"The Germans ... employed ... precautions. It was forbidden to transmit the same message a second time after an error had been made; the text had to be reedited, without altering the content, of course."* Der Weg zum Untergang der Wehrmacht war auch mit manchen guten Absichten gepflastert.

2.1.1 Ohnehin darf das Chiffrier- und Dechiffrierverfahren nicht zu kompliziert sein: Es muß dem jeweiligen Personenkreis, was dessen Intelligenz und Lebensumstände anbelangt, angemessen sein. Am geringsten sind die Ansprüche hier auf militärischem Gebiet im taktischen Fronteinsatz. Dann kommt sofort das Feld der Diplomatie, jedenfalls wenn man darauf besteht, daß der Botschafter selbst die Ver- und Entzifferung vornimmt. Als *Wheatstone* 1854 dem Unterstaatssekretär des britischen Foreign Office das heute als PLAYFAIR bekannte Verfahren demonstrierte (s. 4.2) und dabei sagte, das könnten drei von vier Knaben der nächstgelegenen Volksschule erlernen, bemerkte dieser trocken "*that is very possible, but you could never teach it to attachés*"!

Auch ist zu bedenken, daß manche Nachricht nicht länger geheimgehalten werden muß, bis das mitgeteilte, beabsichtigte oder stattgefundene Ereignis ohnehin offenkundig geworden ist. Diplomatische Nachrichten geheimzuhalten, kann allerdings noch nach Jahrzehnten geboten sein. Unübertrefflich in dieser Hinsicht und hinsichtlich des Schleiers, den sie über ihr Chiffrierwesen legen, sind die Briten, von den Russen ganz zu schweigen. Jedenfalls kommt es nur darauf an, zu wissen, wie lange der **unbefugte Entzifferer** (engl. *unauthorized decipherer*) mindestens zu tun hat, um die Nachricht herauszulesen – die Chiffre zu „brechen" – und es ist dann nicht nötig zu behaupten, ein gewisses Verfahren sei absolut sicher. Ein von den Deutschen 1917 an der Westfront verwendeter Code (von den Franzosen KRUSA genannt, weil alle Codegruppen mit einem dieser fünf Buchstaben begannen) war solcherart auf ‚geplante Veralterung' angelegt – die Franzosen hatten allerdings meist nach vierzehn, manchmal nach zwei Tagen den Code, der alle Monate wechselte, herausgefunden.

Die quantitative Bewertung der Sicherheit der Verfahren wurde jedoch erst durch die bahnbrechenden Ideen von *Claude E. Shannon* (s. Anhang *Perfekte Sicherheit und praktische Sicherheit*) möglich. Wie wenig tief das Wissen um die Brauchbarkeit der Methoden noch im 1. Weltkrieg ging, zeigte sich darin, daß 1914 der deutsche Generalstab, als *Le Matin* publizierte, daß Frankreich ‚mitlesen' würde, sein Chiffrierverfahren am 18. November radikal änderte. Der Übergang von sog. doppelter Spaltentransposition (s. 6.2.4) zu einem VIGENÈRE mit Schlüssel *A B C* (s. 8.1.2) und nachfolgender Spaltentransposition war eine *complication illusoire* für das französische Dechiffrierbüro.

Ganz sicher glaubten sich ihrer Sache auch die Liebespaare zu sein, die im London von 1850 in chiffrierten Zeitungsannoncen ihre Gefühle austauschten; eine gewisse Londoner Gesellschaft machte sich jedoch ein Vergnügen daraus,

‚mitzulesen', darunter (s. 2.4.1) *Babbage* sowie *Wheatstone* und *Playfair*, die in einen solchen Liebes-Brief-Wechsel mit einer eigenen, geeignet chiffrierten Nachricht ‚einbrachen' und die Reaktion "*Dear Charlie: Write no more. Our cipher is discovered*" der jungen Dame hervorriefen. Übrigens, trotz – oder vielleicht aufgrund – *Shannon*'s verdienstvoller Aufklärung sollen noch heute in Londoner Tageszeitungen verschlüsselte Anzeigen zu finden sein.

Eine andere Dame fand sich gar zutiefst beeindruckt von einem Mann, dem sie ein Rezept, Gold zu machen, übergeben hatte, das chiffriert war und wozu sie allein den Schlüssel wußte – als er ihr nicht nur mitteilte, daß er es entziffert hatte, sondern ihr auch das Schlüsselwort nannte. Der Mann mußte hexen können, mußte *Gedanken lesen* können, dachte sie und schloß ihn folglich lieber gleich ganz in ihr Herz. Es war, 1757, die wohlhabende *Madame d'Urfé*, und der Kavalier, der sie übrigens bald verließ, war – *Giacomo Girolamo Casanova, Chevalier de Seingalt* (1725–1798), dessen kryptanalytische Beflissenheit offenbar nicht so weithin bekannt ist wie seine sonstigen Vorzüge.



Casanova



Abb. 18. Verschlüsselungssystem der Reifenhersteller

Reifen-Zeichen

(1) tubeless bedeutet schlauchlos

(2) 175 ist die Breite des Reifens in mm
S steht für zulässige Höchstgeschwindigkeit (bis zu 180 km/h im Falle von Sommerreifen)
R bedeutet Radialreifen (leer: Diagonalreifen)
14 ist der Durchmesser der Felge in inches

(3) TWI (tread wear indicator) weist auf den Profilabnutzungsanzeiger hin (sechs Querstege in den Profilrillen treten bei 1.6 mm Restprofil auf)

(4, 5) europäische Reifenkennzeichnungen:
88 codiert die maximale Last pro Rad
S steht für Geschwindigkeit bis zu 180 km/h

(6) Karkasse aus 2 Lagen Kunstseide

(7) Gürtel aus 2 Lagen Stahl und Kunstseide

(8) maximaler Luftdruck in Pfund/Quadratzoll (gilt nur für U.S.A.)

(9) maximale Last pro Rad in Pfund (gilt nur für U.S.A.)

(10) Hersteller

(11, 12) Zertifikat der Bauartprüfung: 4 ist der Code für das Land in dem die Bauartprüfung durchgeführt wurde (hier Holland).

(13) Zertifikat des DOT (Department of Transportation, das US Verkehrsministerium)

(14) Hersteller-Code: LM = Fabrik; J3 = Größe; MEB = Typencode; 344 = Datumscode (34. Produktionswoche von 1974)

Auch *Marie Antoinette* wußte Liebe und Kryptographie zu verbinden, ebenso der britische König *Eduard* VIII. So hat die Kryptographie neben diplomatischen und militärischen auch ihre zivilen und privaten Anwendungen, ganz

zu schweigen von den kommerziellen, etwa der Kaufmanns-Chiffre zur Preisauszeichnung und der (jetzt abgeschafften) verschlüsselten Angabe des Abpackungsdatums der Butter (s. 3.1.1) oder dem Verschlüsselungssystem der Reifen-Hersteller (Abb. 18). Amüsante Geschichten gibt es auch über die angebliche Unbrechbarkeit einer Chiffrierung. Von der Überschätzung der eigenen Klugheit profitiert regelmäßig die Gegenseite. Ein Beispiel solcher Übertreibung ist es, wenn von *Paul Schilling von Cannstatt*, einem der Erfinder des elektromagnetischen Telegraphen (1832) gesagt wird, er „stellte für das russische Ministerium ein so geheimes Alphabet zusammen, die sogenannte Chiffre, daß sogar ein derart ausgeklügeltes Geheimkabinett wie das österreichische es in 50 Jahren nicht durchlesen wird" (*F. P. Fonton*, nach *A. V. Jarozkij*). Und noch 1917 wurde in dem so angesehenen *Scientific American* die VIGENÈRE-Methode (s. 7.4) als unbrechbar bezeichnet.

Eine besondere Ironie des Schicksals wollte es, daß *Étienne Bazeries*, der große französische Kryptologe (1846–1931), der eine ganze Reihe von sogenannten unbrechbaren Chiffrierverfahren, die dem französischen Sicherheitsbüro vorgelegt worden waren, niedergeschmettert hatte, schließlich selbst vermessen genug war zu glauben, er habe ein absolut sicheres Verfahren (≪*Je suis indéchiffrable*≫, Abb. 19) gefunden. Es bereitete seinem Gegenspieler, dem *Marquis de Viaris* – der erste moderne Kryptologe übrigens, der die Mathematik ins Spiel brachte – kein geringes Vergnügen, sich zu rächen und einige Chiffren, die *Bazeries* ihm sandte, zu brechen (s. 7.5.3, 14.3).



Abb. 19. *Bazeries*' Zylinder mit der Nachricht ≪je suis indéchiffrable≫

2.1.2 Ein lukrativer Seitenast der Kryptographie ist die Erfindung und finanzielle Auswertung von Chiffrier- und Dechiffriermaschinen. Bis zum 19. Jahrhundert waren es mechanische Geräte, seit Beginn des Jahrhunderts setzte auch hier die Automatisierung, später die Elektronisierung und neuerdings die Mikrominiaturisierung ein. Ende 1939 betätigte sich auch der am Westwall stationierte Gefreite *Konrad Zuse* als Erfinder eines Chiffriergerätes, eines Zusatzgerätes zu einem Fernschreiber. Er konnte allerdings das Heereswaffenamt für seine Erfindung, die eine Vernam-Chiffrierung (s. 8.3.2) enthielt, nicht gewinnen: Man gab ihm zu verstehen, „daß man bereits über gute Geräte dieser Art verfüge". Dabei handelte es sich nicht, wie *Zuse* später fälschlich meinte, um die ENIGMA, sondern um SZ 40 und T 52 (s. 9.1).

Mikrorechner – von Größe, Gewicht und Preis eines Taschenrechners – können heute die Leistungen der besten Chiffriermaschinen des 2. Weltkriegs er-

bringen. Damit ist die frühere Bedeutung guter Verfahren, die durch das Vorhandensein ‚riesengroßer' Rechner in den kryptanalytischen Zentralen stark abgewertet worden sind, nicht nur wiederhergestellt worden: Es kann mit einem handelsüblichen Mikrorechner der $ 100-Klasse und erst recht mit einem PC (*Personal Computer*) auch eine weitaus komplexere Chiffrierung vorgenommen werden, als es die klassischen Maschinen zustandebrachten.

Im übrigen muß man bei der Beurteilung eines auf Unterlagen irgendwelcher Art gestützten Verfahrens, also auch eines maschinellen Verfahrens, damit rechnen, daß diese Unterlagen in *gegnerische* Hände fallen können (*Shannon's* Maxime, s. 11.2.3). Ein lediglich mit einer Diskette gefütterter Mikrorechner hat aber keinerlei „verräterische" kryptographische Struktur — außer vielleicht Alphabettastatur und Buchstabenanzeige.

Bei den sogenannten öffentlichen Schlüsseln (engl. *public keys*), die heute für kommerzielle Verbindungen propagiert werden, werden das Chiffrier- und das Dechiffrierverfahren sogar veröffentlicht, lediglich der Schlüssel zum Dechiffrieren bleibt geheim; *Shannon's* Maxime wird also auf die Spitze getrieben (s. 10.1.2). Dabei führt der zunehmende Gebrauch offener Nachrichtenwege dazu, daß neben die klassische Geheimhaltung die Authentisierung als erklärtes Ziel der Kryptographie tritt (s. 10.5, 10.6).

2.1.3 Die Literatur bedient sich gelegentlich kryptologischer Techniken. Schwierige, dicht verwobene literarische Werke wie *Zettels Traum* von *Arno Schmidt* (1970) wollen „entziffert" werden.

Ein besonderes Problem stellen die **angeblichen Geheimtexte** dar. *Balzac* hat in *La physiologie du mariage* (1829) eine Stelle ≪*La Bruyère a dit très spirituellement: 'C'est trop contre un mari que la dévotion et la galanterie: une femme devrait opter.' L'auteur pense que La Bruyère s'est trompé. En effet:* ··· ≫. Was danach kommt, ist ein Mischmasch durcheinandergepurzelter Buchstaben, so als ob ein Setzkasten ausgeschüttet worden wäre. In der Tat finden sich in vier Auflagen — darunter wenigstens drei zu Lebzeiten von *Balzac* — vier *verschiedene* solcher Texte. *Balzac* hat sich wohl einen Scherz geleistet. Nichtsdestotrotz untersuchte *Bazeries* ein solches Kryptogramm 1901 gründlich und fand, daß es in kein bekanntes System paßte, daß es ≪*une facétie de l'auteur*≫ sei.

Viel Aufregung gab es, seit *Ignatius Donelly*, amerikanischer Provinzpolitiker und einfallsreicher pseudowissenschaftlicher Kopf, der schon über Atlantis und den Zusammenstoß der Erde mit einem Meteor spekuliert hatte, sich 1878 daran machte, in *Shakespeare*'s Werk steganographische Hinweise, daß *Sir Francis Bacon* der Autor sei, zu finden. (Dieser Chimäre jagte auch *Georg Cantor*, der Erfinder der modernen Mengenlehre, längere Zeit nach.) Nun kann man aus einem genügend langen Text, wenn man nur genügend viele Zeichen als belanglos erklärt (und vielleicht auch noch die verbleibenden Zeichen permutiert) alles herauslesen — man nehme nur die hypothetische Nachricht *Lord Byrons* in 1.6. So gelangen auch *Donelly* einige scheinbare Erfolge. Eine

Flut von Amateuren schloß sich an. Das wäre alles nicht bemerkenswert, wäre nicht ein *William Frederick Friedman*, der Genetik studiert hatte, 1915 von einem reichen Textilhändler und Mäzen namens *George Fabyan* angeheuert worden, der neben einem biologischen, einem chemischen und einem akustischen Laboratorium auch Kryptologen beschäftigte, die nachweisen sollten, daß *Bacon Shakespeare* sei. *Friedman*[3] fand dort Interesse an *Elizebeth Smith*, einer jungen Kryptologin, und an der Kryptologie. Er verheiratete sich mit beiden und wurde der erfolgreichste amerikanische Kryptologe.

2.1.4 Die amtlichen kryptologischen Dienste führen zeitgemäß im 20. Jahrhundert geheimnisvoll klingende Namen. Meistens sind sie eingebettet in die allgemein mit der Beschaffung von Nachrichten und mit der Spionage-Abwehr außerhalb des eigenen Landes befaßten Geheimdienste. An der Spitze der Berühmtheit steht M.I.6, der *(British) Secret Intelligence Service* (S.I.S.) in Großbritannien, direkt dem *Foreign Office* unterstellt, daneben steht M.I.8, *Signals Intelligence Service*. In den U.S.A. gibt es seit 1947 C.I.A., die *Central Intelligence Agency*, die zusammen mit der *Defense Intelligence Agency* (D.I.A.) dem *U.S. Intelligence Board* (U.S.I.B.) untersteht und damit von Legislative und Exekutive kontrolliert wird. In Nachkriegsdeutschland ist der Bundesnachrichtendienst (BND), dem Bundeskanzleramt direkt unterstellt, zu nennen. Das postkommunistische Rußland hat den Sicherheitsdienst FSB.

Die eigentlichen kryptologischen Dienste, insbesondere die kryptanalytischen Sonderabteilungen, sind häufig zwischen Diplomatie und Militär aufgeteilt. Das mag organisatorisch gut begründet sein, hindert jedoch oft den Erfahrungsaustausch. In Großbritannien wurden im 2. Weltkrieg die Admiralität (O.I.C., *Operational Intelligence Center*) und das *Foreign Office* (*Department of Communications*) durch die verzweifelte Situation von 1940 zu enger Zusammenarbeit gezwungen; *Churchill* tat ein übriges und richtete mit der ihm direkt unterstellten *London Controlling Section* (L.C.S.) eine schlagkräftige, von Oberst *John Henry Bevan* geleitete Überbehörde ein. Für die Kryptanalyse war innerhalb M.I.8 zuständig G.C.H.Q. (*Government Communications Headquarters*), mit allerlei, teils historisch begründeten Spitznamen: G.C. & C.S. (*Governmment Code and Cypher*[4] *School*), War Station, Station X, Room 47 Foreign Office; häufig nach dem Ort, an dem es sich seit 1939 befand, BP (*Bletchley Park*) genannt. Auch in BP blieb eine gewisse Trennung von AI (*Air Intelligence*) und MI (*Military Intelligence*) von der traditionsbewußten Navy aufrechterhalten. Beide blickten auf ihre Erfolge im 1. Weltkrieg zurück, die in der M.I.1(b) (*Military Intelligence Division*) des *War Office* und im *Room 40* der *Admiralty* errungen worden waren.

In den Vereinigten Staaten von Amerika stellte sich im 1. Weltkrieg nach dem Kriegseintritt 1917 eine Notwendigkeit zum raschen Ausbau der militärischen Kryptologie ein. Im Rahmen der A.E.F. (*American Expeditionary Forces*)

[3] Geb. 24. 9. 1891 in Kischinew (Bessarabien) als *Wolfe Friedmann*, gest. 2. 11. 1969, bestattet in Arlington, Virginia (U.S.A.). Die Familie war 1892 nach den U.S.A. emigriert.

[4] *cypher* ist eine veraltete, in Großbritannien noch verbreitete Schreibweise für *cipher*.

fand sich G.2 A.6 (*General Staff, Military Intelligence Section, Military Information Division, Radio Intelligence Section*) mit der *Code Compilation Section of the Signal Corps*; unter den Augen der MI-8 (Kryptologische Sektion der *Military Intelligence Division*), geleitet von *Herbert Osborne Yardley* (1889–1958). Eine Rivalität zwischen Army und Navy zog sich durch den 2. Weltkrieg: OP-20-G war die kryptologische Organisation der *Navy* mit der kryptanalytischen Abteilung OP-20-GY, *Signal Intelligence Service* (SIS) war das Gegenstück der *Army*, das *Yardley* aufgebaut hatte und das seit 1929 von *William Friedman* geleitet wurde. Nach den Erfahrungen des 2. Weltkriegs wurde eine Konzentration herbeigeführt: Innerhalb G-2 entstand 1945 durch Verschmelzung der *Army Signal Security Agency* und der Kryptanalysis des *Signal Corps* die A.S.A. (*Army Security Agency*), dann 1949 die A.F.S.A. (*Armed Forces Security Agency*) und weiterhin unter dem *Secretary of Defense* 1952 die N.S.A. (*National Security Agency*), die unter die Leitung des legendären *Bobby Ray Inman* kam. Eine wichtige Einrichtung ist I.D.A., das *Institute for Defense Analyses*, das offener arbeitet und mit einigen Universitäten Fühlung hat, sowie die *Defense Intelligence Agency* unter den *Joint Chiefs of Staff.*

Auch im Deutschen Reich waren die Dienste zersplittert: Auswärtiges Amt einerseits, Heer und Kriegsmarine andrerseits erfuhren im 2. Weltkrieg noch Konkurrenz durch die Luftwaffe und durch den Sicherheitsdienst. Zwar war auf Betreiben des späteren Generals *Erich Fellgiebel* (1886–1944) schon 1934 mit der ENIGMA eine Vereinheitlichung der maschinellen Kryptographie erreicht worden, aber die vom OKW beständig geforderte Koordinierung aller Arbeiten scheiterte noch im Herbst 1943 am Widerstand von *Ribbentrop, Göing* und *Himmler*. Als im November 1944 schließlich die Koordinierung durch WNV/Chi (Wehrmachtnachrichtenverbindungen Chiffrierwesen) durch Führerbefehl angeordnet wurde, war das Nachrichtenwesen bereits in den Händen des aufstrebenden, *Himmler* und *Hitler* stets treue Ergebenheit heuchelnden, vom SS Brigadeführer zum SS Obergruppenführer aufgerückten *Walter Schellenberg* (1910-1952), der nach Verbüßung seiner in den Nürnberger Prozessen verhängten Strafe von nur sechs Jahren an einem Leberleiden starb — die Modeschöpferin *Coco Chanel* bezahlte seine Beerdigung.

Im Nachkriegsdeutschland wurde 1953 in Bad Godesberg die ‚Bundesstelle für Fernmeldestatistik' eingerichtet, deren Deckname eine leichte Untertreibung war; mit dem wahren Namen „Zentralstelle für das Chiffrierwesen" war sie eine kryptanalytische Unterabteilung des Bundesnachrichtendienstes. Seit 1990 besteht neben dem nicht in der Öffentlichkeit wirkenden ‚Amt für Militärkunde' ein „Bundesamt für Sicherheit in der Informationstechnik" (BSI) im Innenministerium, das Fragen der öffentlichen Kryptologie zugewandt ist. In Frankreich war 2bis (eine Hausnummer in der Avenue de Trouville) *nom de guerre* für die kryptanalytische Abteilung des *Deuxième Bureau.* In Schweden lief das kryptanalytische Büro *Försvarets Radioanstalt* unter der Abkürzung FRA, in Italien war es SIM (*Servizio Infomazione Militare*); in Japan ist

toku mu han („Spezial Aufgaben Abteilung“) das Wort für die 1925 im Admiralstab eingeführte kryptanalytische Abteilung, daneben *angō kenkyū han* („Chiffrier Forschungs Abteilung“) für die des Außenministeriums.

2.2 Chiffrierung

Fassen wir zusammen: Die **Kryptologie** (engl. *cryptology*) ist die Wissenschaft von den (offenen) Geheimschriften (**Kryptographie**), von ihrer *unbefugten Entzifferung* (**Kryptanalyse**, engl. *cryptanalysis*) und von den Vorschriften, die dazu dienen sollen, die unbefugte Entzifferung zu erschweren (**Chiffriersicherheit**, engl. *cryptanalytical security*).

2.2.1 Der Zeichenvorrat V, mit dessen Hilfe der **Klartext** (engl. *plain text*[5]) formuliert wird, ist das **Klartextvokabular** oder der **Klartextzeichenvorrat**.

Der Zeichenvorrat W, mit dessen Hilfe der **Geheimtext** (‚Decktext‘, engl. *cipher text*, *code text*) formuliert wird, ist das **Geheimtextvokabular** oder der **Geheimtextzeichenvorrat**, kurz auch **Chiffre** oder **Code**. Die einzelnen Zeichen aus W (**Chiffren-, Codezeichen**) können auch **Sigel**[6] sein.

V und W können verschieden sein, können aber auch zusammenfallen. V^*, W^* sei die Menge der Wörter über V, W (**Klartextwörter**, **Geheimtextwörter**). V^* heißt **Klartextraum**, W^* heißt **Geheimtextraum**. ε bezeichne das leere Wort. Z^n ist die Menge aller Wörter der Länge n über Z, $Z^{(n)}$ bezeichnet $\{\varepsilon\} \cup Z \cup Z^2 \cup Z^3 \ldots \cup Z^n$.

V und W sind in allen praktischen Fällen (nichtleere) endliche Mengen. Man kann aber theoretisch auch abzählbar unendliche Mengen zulassen, denn auch dann sind V^* und W^* abzählbar unendlich.

2.2.2 Eine **Chiffrierung** wird definiert als eine Relation $\mathbf{X} : V^* \dashrightarrow W^*$. Die konverse Relation $\mathbf{X^{-1}} : V^* \dashleftarrow W^*$, definiert durch

$x \leftarrow\!\dashv y$ genau dann, wenn $x \mapsto y$, wird **Dechiffrierung** genannt.

Man definiert $\mathcal{P}_y = \{x \in V^* : x \overset{\mathbf{X}}{\mapsto} y\}$ als **Linksfaser** von $y \in W^*$,

$\mathcal{H}_x = \{y \in W^* : x \overset{\mathbf{X}}{\mapsto} y\}$ als **Rechtsfaser** von $x \in V^*$.

Der befugte Empfänger einer chiffrierten Nachricht sollte den Klartext eindeutig zurückgewinnen können. Eine Chiffrierung ist deshalb in der Regel **injektiv**: für alle $y \in W^*$ ist $\mathcal{P}_y$ einelementig oder leer.

Injektiv bedeutet: $(x \mapsto z) \wedge (y \mapsto z) \Rightarrow (x = y)$ (‚linkseindeutig’).

In der Regel wird auch gefordert, daß die Chiffrierung $\mathbf{X}$ **definal** (eine Abbildung) ist, d.h. daß für alle $x \in V^*$ $\mathcal{H}_x$ nicht leer ist.

---

[5] Engl. *clear text* bedeutet: unchiffriert übermittelter Text.

[6] Von lat. *sigillum* ‚Zeichen‘ (engl. *siglum*): abkürzende Sonderzeichen wie §, &, %, $, #, @; auch in der Stenographie (‚Kürzel‘) und im Journalismus (‚r.s.‘ für Theodor Heuss).

Ist die Relation $\dashrightarrow$ auch **funktional** (‚rechtseindeutig'):

für alle $x \in V^*$ ist $\mathcal{H}_x$ einelementig oder leer,

so ist $\mathbf{X}: \ V^* \dashrightarrow W^*$ sogar eine **Funktion** $V^* \longrightarrow W^*$ und, falls surjektiv, eine **eineindeutige Zuordnung** $V^* \longleftrightarrow W^*$.

Man erhält die Durchführung einer Chiffrierung $\mathbf{X}: \ V^* \dashrightarrow W^*$ durch einen nichtdeterministischen Auswahloperator η , $\mathbf{X}(x) = \eta\, \mathcal{H}_x$.

Ist die Menge $\mathcal{H}_x$ nicht einelementig und nicht leer, so heißen ihre Elemente **homophone** Texte für x. Homophone Texte sind also solche verschiedene Geheimtextwörter, die in der Relation $\dashrightarrow$ dem selben Klartextwort zugeordnet sind. **Polyphone** Texte sind solche verschiedene Klartextwörter, die in der Relation $\dashrightarrow$ dem selben Geheimtextwort zugeordnet sind.

Im *funktionalen* Fall gibt es keine homophonen Texte, die Chiffrierung ist deterministisch, und also eine eindeutige Abbildung des Klartextbereichs der Relation in den Geheimtextbereich.

In der Regel gilt $\varepsilon \overset{\mathbf{X}}{\mapsto} \varepsilon$. Enthält $\mathcal{H}_\varepsilon$ auch von ε verschiedene Elemente, also homophone Texte für $\varepsilon \in V^*$, so heißen diese **Blendtexte**.

Beachte, daß die Menge aller Chiffrierungen $V^* \dashrightarrow W^*$ (bei festen nichtleeren V, W) überabzählbar ist.

Eine Chiffrierung $\mathbf{X}: \ V^* \dashrightarrow W^*$ soll **endlich** heißen, wenn die Menge aller in Relation stehenden Paare eine endliche Menge ist. Es ist dann für geeignete n, m $\quad \mathbf{X}: \ V^{(n)} \dashrightarrow W^{(m)}$.

Wie aber legt man eine Relation $V^* \dashrightarrow W^*$ fest, wie gibt man sie an? Selbst wenn sie endlich ist, kann es sich praktisch verbieten, die Paare aufzulisten. Man verwendet daher gern eine induktive Festlegung.

2.3 Chiffrierschritt-System

Es sei M , das **Chiffrierschritt-System**, eine nichtleere, in der Regel *endliche* Menge $\{\chi_0 \ , \ \chi_1 \ , \ \chi_2 \ , \dots , \ \chi_{\theta-1}\}$ von (injektiven) Relationen $\chi_i : V^{(n_i)} \dashrightarrow W^{(m_i)}$. Jedes χ_i heißt **Chiffrierschritt**.

Eine Chiffrierung $\mathbf{X} = [\ \chi_{i_1} \ , \ \chi_{i_2} \ , \ \chi_{i_3} \ , \ \dots\ ]$ heißt **endlich erzeugt** (mittels des Chiffrierschritt-Systems M), wenn sie durch eine (abbrechende oder unendliche) Folge $(\chi_{i_1} \ , \ \chi_{i_2} \ , \ \chi_{i_3} \ , \ \dots\ )$ von Chiffrierschritten $\chi_i \in M$ unter der Konkatenation $.\!\star\!.$ **induziert** wird, d.h.

$x \overset{\mathbf{X}}{\mapsto} y$ gilt für $x \in V^*$, $y \in W^*$ genau dann, wenn es Zerlegungen $x = x_1 \star x_2 \star x_3 \star \dots \star x_k$ und $y = y_1 \star y_2 \star y_3 \star \dots \star y_k$ gibt[7] mit

$$x_j \overset{\chi_{i_j}}{\mapsto} y_j \ \text{ für } \ j = 1 \ , \ 2 \ , \ \dots \ k \ .$$

---

[7] Dabei soll jedes Wort aus V^* durch Anfügung belangloser Zeichen geeignet aufgefüllt gedacht werden.

Beispiel:

$\chi_i : V^{(n_i)} \dashrightarrow V^{(n_i)}$ ist zyklische Transposition von n_i Elementen $(\theta = 4)$;
$n_1 = 3,\ n_2 = 5,\ n_0 = 2,\ n_3 = 6$

$$\frac{\text{e s w}}{\text{s w e}}\ \frac{\text{a r s c h}}{\text{r s c h a}}\ \frac{\text{o n}}{\text{n o}}\ \frac{\text{d u n k e l}}{\text{u n k e l d}}\quad (\chi_1\ ,\ \chi_2\ ,\ \chi_0\ ,\ \chi_3)$$

2.3.1 $\theta = |M|$ soll stets die **Kardinalität** des Chiffrierschritt-Systems bezeichnen. Ein Chiffrierschritt $\chi_i : V^{(n_i)} \dashrightarrow W^{(m_i)}$ ist eine **erzeugende Relation** der Chiffrierung, die Zahl n_i heißt die (maximale) **Chiffrierbreite**, die Zahl m_i die (maximale) **Chiffratbreite** von χ_i . Die Relation χ_i kann nichtdeterministisch sein. Das Chiffrierschritt-System und die Chiffrierung heißen **endomorph**, falls $V = W$.

Wenn man von **Homophonen** (engl. *homophones*, auch *variants*, *optional substitutes*, *multiple substitutes*, frz. *représentations multiples*) und **Blendern, Nieten, Füllzeichen, Blindsignalen** (engl. *nulls*, auch *dummies*, frz. *nonvaleurs*) spricht, meint man meist die des Chiffrierschrittes. Enthält der Geheimtextbereich des Chiffrierschritts Wörter verschiedener Länge, so heißt der Chiffrierschritt **gespreizt**.

Die Injektivität der erzeugten Chiffrierung ist nicht ohne weiteres gegeben: Sei etwa

$$\begin{aligned} \text{a} &\mapsto \cdot - \\ \text{i} &\mapsto \cdot\cdot \\ \text{l} &\mapsto \cdot - \cdot\cdot \end{aligned}$$

aus einem injektiven $V^1 \longrightarrow W^{(4)}$, so gilt in $V^* \dashrightarrow W^*$

$$\text{ai} \mapsto \cdot - \cdot\cdot \quad \text{und} \quad \text{l} \mapsto \cdot - \cdot\cdot \ ,$$

es ist also die Injektivität verletzt (gute Funker setzen deshalb klare Pausen).

2.3.2 Ein Chiffrierschritt $\chi_i : V^{(n_i)} \dashrightarrow W^{(m_i)}$ ist (bei endlichen V und W) wesensgemäß endlich, er kann prinzipiell durch Auflistung angegeben werden (**Chiffrentabelle**). Eine tatsächliche Auflistung wird oft als **Codebuch** (frz. *code*, Gesetzbuch) oder **Satzbuch** bezeichnet, der Chiffrierschritt dann als **Codierschritt**. Die terminologische Grenze zwischen ‚Chiffrierung' und ‚Codierung' ist fließend und häufig historisch bestimmt (s. 4.4). Die Ausdrücke ‚Chiffre' und ‚Code' werden auch für die Elemente von $W^{(m_i)}$ verwendet.

2.3.3 Eine mittels M endlich erzeugte Chiffrierung $\mathbf{X} = [\chi_{i_1}\ ,\ \chi_{i_2}\ ,\ \chi_{i_3}\ ,\ \ldots]$ heißt **monoalphabetisch**, wenn sie lediglich einen einzigen Chiffrierschritt (‚Alphabet') umfaßt oder benutzt. Andernfalls heißt sie **polyalphabetisch**. (Ist M einelementig $(\theta = 1)$, so ist jede mittels M endlich erzeugte Chiffrierung monoalphabetisch).

2.3.4 Eine endlich erzeugte Chiffrierung heißt **monographisch**, falls alle n_i der verwendeten Chiffrierschritte gleich 1 sind, **polygraphisch** sonst.

2.3.5 In einem besonders für maschinelle Durchführung wichtigen Spezialfall sind alle Chiffrierschritte aus M von gleicher maximaler Chiffrierbreite n und gleicher maximaler Chiffratbreite m . M umfaßt dann notwendigerweise eine endliche Menge von Chiffrierschritten. Gilt sogar für alle χ_i aus M

$$\chi_i : \ V^n \dashrightarrow W^m \ ,$$

sind also insbesondere alle Chiffrierschritte ungespreizt, heißt die Chiffrierung $[\chi_{i_1}\ ,\ \chi_{i_2}\ ,\ \chi_{i_3}\ ,\ \ldots]$ **Blockchiffrierung** (engl. *block cipher*), ein Wort aus V^n heißt **Block** der Chiffrierung. Selbstverständlich kann die Blockchiffrierung in einem geeigneten Zeichenvorrat von Zeichen-n-tupeln theoretisch als mono*graphisch* aufgefaßt werden.

Chiffrierschritt-Systeme mit $\chi_i : V^n \dashrightarrow W^m$ liefern für $n = 2,\ 3,\ 4,\ 5$ **Bigramm-, Trigramm-, Tetragramm-, Pentagrammchiffrierungen**, die für $m = 2,\ 3$ **bipartit, tripartit** (engl. *bipartite, tripartite*, frz. *bifide, trifide*) heißen. Häufig wählt man überdies $V = W$ und $m = n$ und hat dann eine **Blockchiffrierung im engeren Sinn**.

2.3.6 Ein **Strom** $(z_1, z_2, z_3, \ldots)$ ist eine unendliche Folge von Zeichenblöcken. Einem Strom ist eineindeutig zugeordnet $((z_1), (z_1 \star z_2), (z_1 \star z_2 \star z_3), \ldots)$, eine unendliche Folge von Wörtern, den **Abschnitten** $(z_1 \star z_2 \star \ldots \star z_i)$ des Stroms.

Als **Klartextstrom** wird eine unendliche Folge von Blöcken $(p_1, p_2, p_3, \ldots)$, wo $p_j \in V^n$, bezeichnet; entsprechend eine unendliche Folge von Blöcken $(c_1, c_2, c_3, \ldots)$, wo $c_j \in W^m$, als **Geheimtextstrom**. Eine **Stromchiffrierung** (*stream cipher*) ist eine Blockchiffrierung von Abschnitten eines fiktiven Klartextstroms zu Abschnitten eines ebenso fiktiven Geheimtextstroms.

Eine mittels M endlich erzeugte Stromchiffrierung $\mathbf{X} = [\chi_{i_1}\ ,\ \chi_{i_2}\ ,\ \chi_{i_3}\ ,\ \ldots]$ heißt **periodisch** (engl. *repeated key*) bzw. **fortlaufend** (‚aperiodisch', engl. *running key*), jenachdem ob die unendliche Folge $(\chi_{i_1}\ ,\ \chi_{i_2}\ ,\ \chi_{i_3}\ ,\ \ldots)$ schließlich periodisch ist oder nicht. Eine monoalphabetische Chiffrierung ist trivialerweise periodisch. Eine fortlaufende Chiffrierung ist also notwendigerweise polyalphabetisch. Darauf wird in 8.7 und 8.8 näher eingegangen werden.

Jede periodische Blockchiffrierung der Periode r kann selbstverständlich theoretisch auch als mono*alphabetisch* aufgefaßt werden, mit

$$\chi_0 \ : \ V^{n\cdot r} \dashrightarrow W^{m\cdot r}$$

als einzigem Chiffrierschritt. Für fortlaufende Chiffrierungen gilt dies nicht; sie gehören prinzipiell einer mächtigeren Klasse von Chiffrierungen an: Ordnet man jedem χ_i aus der endlichen Menge M den Index i zu, so kann die Folge $(\chi_{i_1}\ ,\ \chi_{i_2}\ ,\ \chi_{i_3}\ ,\ \ldots)$ im Zahlsystem zur Basis θ durch den Bruch $0.i_1\, i_2\, i_3\ \ldots$ dargestellt werden. Bei festem M entspricht dann der Menge der periodischen Blockchiffrierungen eine Teilmenge der abzählbaren Menge der rationalen Zahlen; der Menge der fortlaufenden Blockchiffrierungen die überabzählbare Menge der irrationalen Zahlen zwischen 0 und 1 .

Ein aktuelles Beispiel einer monoalphabetischen, polygraphischen Blockchiffrierung ist das vom *National Bureau of Standards* der U.S.A. seit 1977 propagierte DES-Chiffrierverfahren, mit eineindeutigen endomorphen Chiffrierschritten[8] $V^8 \longleftrightarrow V^8$ mit einem Zeichenvorrat $V = Z_2^8$ (2.5.1) von 256 verschiedenen 8-Bit-Wörtern – allerdings nicht durch Auflistung, sondern mit Hilfe eines Algorithmus definiert. Solche algorithmisch definierten Chiffrierungen (s. 9.6) ermuntern nicht gerade zum Gebrauch von Homophonen.

Von einer polyalphabetischen, polygraphischen Chiffrierung, die aber keine Blockchiffrierung ist, kann man sprechen, wenn ein Klartext Wort für Wort mit Hilfe mehrerer, nach irgend einer Vorschrift periodisch oder nichtperiodisch abwechselnder Codebücher chiffriert wird. Praktische Verwendung kann hochkomplexe polyalphabetische polygraphische Blockchiffrierung wohl nur, aber gerade auch unter Verwendung von Rechenanlagen bekommen.

2.4 Polyphonie

Die Verwendung von Homophonen und Blendern gehört seit 1400 zum Standard der Kryptologie. Seit 1500 wird auch von Chiffrierungen mit verschieden langen Chiffren Gebrauch gemacht; die Bedeutung der Linkseindeutigkeitsbedingungen bei gespreizten Chiffrierschritten (3.4) wurde spätestens um 1580 von *G. B.* und *M. Argenti* klar erkannt. Die moderne Fano-Bedingung („keine Chiffre ist Anfang einer anderen Chiffre“, *R. M. Fano*) ist eine hinreichende Bedingung, die die *Argenti*s anscheinend auch schon kannten. Für ungespreizte Chiffrierschritte ist die **Wortfuge** durch Abzählen auffindbar.

2.4.1 Polyphone werden, ohne daß man sich darüber Gedanken macht, in manchen Sprachen verwendet, z.B. im Englischen, wo die beiden Phoneme [ai] wie in [braik] und [i:] wie in [fri:k] in der Schrift durch das selbe Zeichenpaar ea wiedergegeben werden. Kryptographisch haben polyphone Chiffrierschritte, bei denen verschiedenen Klartextwörtern ein und das selbe Geheimtextwort zugeordnet ist, Nachteile: Sie erschweren die Dechiffrierung und sind deshalb selten zu finden. ‘SA Cipher’, ein Code der britischen Admiralität von 1918 (s. 4.4.3, Abb. 37), sowie die Chiffre der Herzogin von *Berry* mit dem Merkvers LEGOUVERNEMENTPROVISOIRE als Substitutionsalphabet (s. 3.2.5), sind einige der wenigen Beispiele für echte Polyphonie. Praktisch ausreichende semantische Entscheidbarkeit liegt vor, wenn etwa die Codewörter „Dieselöl“, „Unteroffizier“, „Paris“, oder „Rollbahn“, „General“, „Bodennebel“ polyphon sind. Am ehesten kommen anscheinend Amateure auf diese Idee. Ein englisches Liebespaar gab *Babbage* 1853 eine Nuß zu knacken durch eine polyphone Chiffre mit den Ziffern 0 bis 9 , wobei

1 für t und u , 2 für m und o , 4 für e und r , 8 für h und i usw.

stand. Die Geheimnachricht begann (mit zwei Chiffrierfehlern) mit

1821 82734 29 30 84541

---

[8] die fest aus 2^{56} Möglichkeiten (Schlüssellänge 56 Bits, s. 9.6.1.1) ausgewählt werden.

was “Thou image of my heart” bedeutete. Es scheint, daß die Liebenden an der Komplikation des Verfahrens besondere Lust empfanden.

Jedoch ist ein polyphones Chiffrierverfahren schon in den Hochkulturen zwischen Nil und Euphrat verwendet worden: Da dort die Buchstabenzeichen gleichzeitig als Zahlenzeichen dienten, wurden gerne die Zahlwerte der Zeichen eines geheimzuhaltenden Wortes zu einer Zahl (‘*gematria*’) zusammengezählt. So könnte das in der Offenbarung des *Johannes* auftretende *isopsephon* 666 (Offb. 13, 18) Kaiser *Nero* bedeuten (Abb. 20). Auf Autoschildern wird 666 als „teuflische Nummer“ mancherorts nicht gern gesehen.

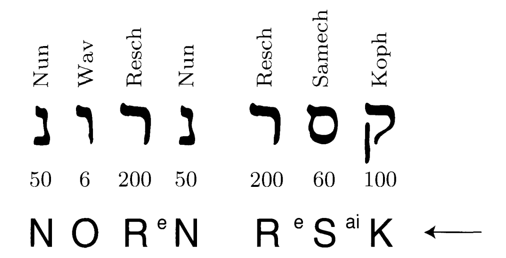
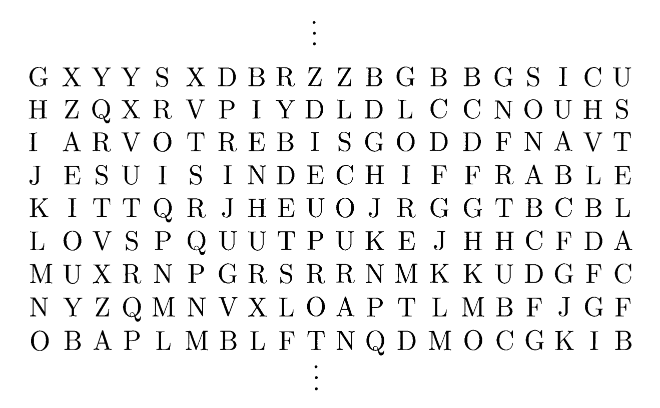


Abb. 20. Zahlwert (hebräisch) von ‚Kaiser *Nero*‘ (nach *Steinbrüggen*)

Von Polyphonie sollte man, von einigen europäischen Sprachen her gesehen, auch bei der Schreibung des Arabischen (ohne Vokale) sprechen. Was aber *“Pthwndxrclzp”* in *James Joyce*’s “Finnegans Wake” bedeuten soll, wird die Literaturwissenschaftler (und die Leichenbestatter) noch lange beschäftigen.

Technisch gesehen, arbeitet *Bazeries*’ Zylinder (Abb. 19), der in 7.5.3 behandelt werden wird, mit Homophonen *und* Polyphonen; die Injektivität wird aber praktisch dadurch hergestellt, daß die ‚illegitimen‘ polyphonen Texte mit an Sicherheit grenzender Wahrscheinlichkeit keinen Sinn ergeben (Abb. 21).

Naive Merkvers-Chiffrierungen (s. 3.2.5) fallen meist polyphon aus. Polyphonie tritt auch bei der unbefugten Entzifferung manchmal erschwerend auf.



⋮

G	X	Y	Y	S	X	D	B	R	Z	Z	B	G	B	B	G	S	I	C	U
H	Z	Q	X	R	V	P	I	Y	D	L	D	L	C	C	N	O	U	H	S
I	A	R	V	O	T	R	E	B	I	S	G	O	D	D	F	N	A	V	T
J	E	S	U	I	S	I	N	D	E	C	H	I	F	F	R	A	B	L	E
K	I	T	T	Q	R	J	H	E	U	O	J	R	G	G	T	B	C	B	L
L	O	V	S	P	Q	U	U	T	P	U	K	E	J	H	H	C	F	D	A
M	U	X	R	N	P	G	R	S	R	R	N	M	K	K	U	D	G	F	C
N	Y	Z	Q	M	N	V	X	L	O	A	P	T	L	M	B	F	J	G	F
O	B	A	P	L	M	B	L	F	T	N	Q	D	M	O	C	G	K	I	B

⋮

Abb. 21. Einige polyphone Texte auf *Bazeries*’ Zylinder

2.4.2 Die Unterdrückung von Wortzwischenräumen und Interpunktionszeichen, die in der klassischen professionellen Kryptographie zu den Grundregeln gehört (man spricht dabei von engl. *formal ciphers*), stellt streng genommen Polyphonie dar. Dabei können allerdings Verwechslungen aufkommen, etwa zwischen „ernsthafte Reformen“ und „ernsthaftere Formen“; der Satz

> „Zehn Finger habe ich an jeder Hand fünf und zwanzig an Händen und Füßen insgesamt“

erlaubt grammatikalisch zwei verschiedene Kommasetzungen. Nur eine gibt auch den rechten Sinn. In dem Satz

> „Er beschloß nicht in den Wald zu gehen“

kann aber nur der situative Kontext über die richtige Kommasetzung entscheiden. Im Englischen ist es noch schlimmer:

> “British Railways hope to have trains running normally late this afternoon”

könnte leicht sarkastisch gedeutet werden, und

> “The Prime Minister called for an end to violence and internment as soon as possible”

ist ein Leckerbissen für die Opposition.

Auch die Verwischung des Unterschieds zwischen Groß- und Kleinbuchstaben kann Verletzung der Injektivität ergeben:

„die gefangenen fliegen“; „der neue weg“.

Für polyphone Texte, die durch das leere Wort chiffriert werden, besteht kaum ein praktisches Bedürfnis, es sei denn, daß inhaltsleeres Gerede oder Geschreibsel eliminiert werden soll.

2.5 Zeichenvorräte

Mit N soll stets $|X|$, die endliche Kardinalität des (Klar- oder Geheimtext-) Zeichenvorrats X, bezeichnet werden. Da der Fall $N = 1$ uninteressant ist, verlangen wir $N \geq 2$. Ein **Alphabet** ist ein linear geordneter Zeichenvorrat.

2.5.1 Die verwendeten Klartext-Zeichenvorräte hängen von der Epoche und von der Sprache ab. Für die auf Hawaii gesprochene Sprache reicht der Zeichenvorrat $Z_{12} = \{\text{a, u, i, o, e, w, h, k, l, m, n, p}\}$ aus.

Im Mittelalter kam man in der lateinischen Tradition anscheinend meistens mit 20 Buchstaben aus, so 1563 *Porta* (Abb. 23)

$$Z_{20} = \{\text{a, b}, \ldots, \text{i, l}, \ldots, \text{t, v, z}\} .$$

Oft wird noch /k/, /x/ und /y/ hinzugenommen oder nur /x/ und /y/ (so anderswo bei *Porta*). Für /w/ wird lange /vv/ geschrieben und so ein Platz gespart, um /& / (*et*) unterzubringen, wie schon auf *Alberti*s Scheibe,

1466 (Abb. 26). Ab 1600 ist dann europäischer Standard ein Alphabet von 24 Zeichen[9] ,

$$Z_{24} = Z_{20} \cup \{\text{k, w, x, y}\}$$

wobei immer noch /v/ für /u/ steht.

Im 18. Jahrhundert wird auch das /u/ mitgenommen,

$$Z_{25}^{uw} = Z_{24} \cup \{\text{u}\}$$

wenn man aber auch das /j/ (im Französischen) verfügbar haben will, muß man das /w/ wieder opfern (*Bazeries*, 1891),

$$Z_{25}^{ju} = Z_{20} \cup \{\text{j, k, u, x, y}\} .$$

Im Italienischen sind /j/, /k/, /w/, /x/, /y/, im Französischen /k/, /w/ sehr selten. Das Irische kommt ohne /j/, /k/, /q/, /v/, /w/, /x/, /y/, /z/ aus. Ab 1900 setzt sich unser heutiges Alphabet

$$Z_{26} = Z_{24} \cup \{\text{j, u}\} .$$

durch. Aber es gibt Ausnahmen. Die Tschechische Exilregierung verwendete im 2. Weltkrieg einen Zeichenvorrat von 31 Buchstaben und 13 Sonderzeichen

$$Z_{44} = \{\text{a, b, c, č, d, e, ě, f}, \ldots, \text{r, ř, s, š, t}, \ldots, \text{z, ž}, \cdot, \ ‚, *, 0, 1, \ldots, 9\} .$$

Das italienische *cifrario tascabile* aus dem 1. Weltkrieg verwendete einen Zeichenvorrat $Z_{36} = Z_{26} \cup \{0,\ 1,\ \ldots,\ 9\}$.

Das (heutige) kyrillische Alphabet hat 32 Buchstaben (ohne Ë):

$Z_{32} = \{$ А Б В Г Д Е Ж З И Й К Л М Н О П
Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я $\}$.

Zur Darstellung von Ziffernzeichen und, wenn nötig, Interpunktionen und diakritischen Zeichen gibt es auch Sonderabmachungen verschiedenster Art. Der Wortzwischenraum wird in der professionellen Kryptographie unterdrückt (er kommt im Deutschen noch häufiger als das /e/ vor).

2.5.2 Die verwendeten Geheimtextzeichenvorräte sind meist durch technische Zwänge bestimmt; es werden dafür neben den obigen Alphabeten auch andere (Abb. 22) benutzt[10], aber auch phantastische Zusammenstellungen, vor allem von Amateuren (s. 3.1.1). **Binär-**, **Ternär-**, **Quinär-**, **Denärchiffrierung** haben $W \mathrel{\hat{=}} Z_2$, $W \mathrel{\hat{=}} Z_3$, $W \mathrel{\hat{=}} Z_5$, $W \mathrel{\hat{=}} Z_{10}$:

Z_{256}	$= Z_2^8$	(Bytes; IBM um 1964)
Z_{32}	$= Z_2^5$	(*Francis Bacon* 1605, 1623, *Baudot* 1874)
Z_{10}	$= \{0, 1, 2, \ldots, 9\}$	(denär)
Z_6	$= \{\text{A, D, F, G, V, X}\}$	(senär; entsprechend den gut unterscheidbaren Morsezeichen ·– , –·· , ··–· , ––· , ···– , –··–)

[9] *Trithemius* (1518) verwendet /w/ als 24. Zeichen. In einer französischen Übersetzung von 1561 (*Gabriel de Collange*) ist das 'deutsche' /w/ wieder durch /&/ ersetzt (nach *Eyraud*).

[10] binär: biliteral, als zweielementiger Zeichenvorrat: *Bacon* 1605, 1623;
dual mit expliziten Werten: $a \mathrel{\hat{=}} 1$, $b \mathrel{\hat{=}} 2$, $c \mathrel{\hat{=}} 4$, $d \mathrel{\hat{=}} 8$, usw.; $abfg \mathrel{\hat{=}} 99$: *Napier* 1617;
dual mit Ziffern, als Stellenwertsystem: *Harriot* vor 1621, *Caramuel* 1670, *Leibniz* 1679.

Z_4	$= \{1, 2, 3, 4\}$	(quaternär; *Alberti* 1466, *Caramuel* 1670, *Weigel* 1673)
Z_3	$= \{1, 2, 3\}$	(ternär; *Trithemius* 1518, *Wilkins* 1641, *Friderici* 1685)
Z_2	$= \{\mathbf{O}, \mathbf{L}\}$	(binär; *Francis Bacon* 1605, 1623)

2.5.3 Die neun Ziffern $\{1, 2, 3, \ldots, 8, 9\}$ dienten (auch iteriert) der Kriegsmarine zur Chiffrierung von Koordinaten in Kartennetzen (Abb. 22).

1	2	3
4	5	6
7	8	9

Abb. 22. Chiffrierung durch Dezimalziffern in Kartennetzen

2.5.4 Fashionable ist die Gruppierung von Geheimtexten in Pentagramme. Sie hat ihren Ursprung in den Tarifbestimmungen der Internationalen Telegraphen-Union, die seit 1875 die Wortlänge auf maximal 10 begrenzte (wobei Codes harten Einschränkungen unterlagen), 1904 aber auch die zulässige Codelänge auf 10 Buchstaben ausdehnte (*Whitelaw's Telegraph Cyphers*: 20 000 aussprechbare Fünfergruppen, daraus 400 000 000 aussprechbare Codewörter) und später generell Fünfergruppen berechnete.

2.5.5 Der unbefugte Entzifferer kennt von der Relation $\mathbf{X}: \ V^* \dashrightarrow W^*$ sowohl V wie $\mathbf{X}$ nicht. Aus $\mathbf{X}(V^*)$ kann er jedoch gelegentlich auf das verwendete Verfahren schließen (*Polybius* etc., s. 3.3.1).

2.5.6 Wenn, wie es häufig der Fall ist, Klartext- und Geheimtextzeichenvorrat zusammenfallen ($V \doteqdot W$, **endomorpher Fall**), ist es heute in theoretischen Abhandlungen weithin üblich, Klartext und Klartextzeichen mit Kleinbuchstaben, Geheimtext und Geheimtextzeichen mit Kapitälchen zu schreiben. Kursive Großbuchstaben stehen dann für sogenannte **Schlüssel** zur Verfügung (Schlüsselzeichen).[11]

2.6 Schlüssel

Schlüssel dienen sowohl der Bildung einzelner Chiffrierschritte wie auch der Auswahl der Chiffrierschritte aus einem Chiffrierschritt-System M. Schlüssel erlauben, die Chiffrierung zu wechseln, nach bestimmten vorher verabredeten Regeln, etwa jeden Tag, oder nach jeder Nachricht. Oft werden Schlüssel so

[11] Auf *Alberti*'s Scheibe (Abb. 26) ist es allerdings anders herum. Auch *Lange-Soudart* zeigen auf einem Saint-Cyr-Schieber (Abb. 27) als Klartextzeichen Großbuchstaben, als Chiffren Kleinbuchstaben.

eingerichtet, daß mit ihrer Hilfe nach einfachen Regeln die einzelnen Chiffrierschritte gebildet werden können. Meistens ist die Abbildung der Menge der Schlüsselzeichen auf die Menge der Chiffrierschritte injektiv, aber es gibt Ausnahmen, wie bei den PORTA-Chiffrierschritten (Abb. 53, Abb. 69), wo je zwei Buchstaben den selben Chiffrierschritt bezeichnen.

Ist k_j der j-te der nacheinander verwendeten Schlüssel, so soll der zugehörige Chiffrierschritt mit χ_{s_j} , $\chi_{s_j} \in \{\chi_0, \chi_1, \chi_2, \ldots, \chi_{\theta-1}\}$ bezeichnet werden.

2.6.1 Der anhaltende Gebrauch des selben Schlüssels kommt der Verwendung eines einelementigen Chiffrierschritt-Systems gleich; die professionelle Kryptographie arbeitet, abgesehen von Codierungen, kaum mit derartigen **festen Chiffrierungen**. Der Gebrauch eines Codebuchs über Jahre hinweg im diplomatischen Verkehr ist ein solcher Fall – man kann allerdings die Diplomaten mancher Staaten kaum als professionelle Chiffrierer ansehen: Diplomatische Codes wurden zuzeiten in Städten wie Wien in einem regen Untergrundmarkt gehandelt. Besonderen Ruf im Stehlen von Codebüchern genoß die Sowjetunion. Im Sommer 1936 entzifferte ein russischer Agent in Haarlem, Niederlande, mit Hilfe eines gestohlenen Codebuches Telegramme zwischen dem japanischen Militärattaché in Berlin und seiner Regierung in Tokyo. Zu Beginn des ersten Weltkrieges besaß vermutlich jede europäische Großmacht Kopien einer oder mehrerer der amerikanischen diplomatischen Codebücher. Und im August 1941 verschaffte *Loris Gherardi* dem italienischen *Servizio Informazione Militare* unbemerkt eine Kopie des BLACK Code, den U.S. Militärattachés gebrauchten.

Vielleicht stimmt auch die von *Allen W. Dulles* erzählte Geschichte von dem amerikanischen Gesandten in Rumänien – wie so häufig ein abgehalfterter Politiker – , der sein Codebuch verloren hatte und den Verlust nicht melden wollte; er ließ immer einige Nachrichten zusammenkommen und nahm dann den Zug nach Wien, um dort in der Botschaft die Arbeit zu verrichten. – Fazit: Auch Codebücher müssen regelmäßig, unter Umständen sogar monatlich, ausgewechselt werden.

Schlüssel, die der Verfahrensauswahl dienen, müssen gegenseitig vereinbart sein. In dieser Vereinbarung liegt oft eine Schwäche der Chiffrierschritt-Systeme. Für exponierte Situationen ist ohnehin der Schlüsselnachschub gefährdet, erschwert oder gar unmöglich. In solchen Fällen greift man oft auf unverfängliches Buchstaben- oder Zahlenmaterial zurück, wie bekannte Romane oder statistische Berichte, Telefonbücher etc. – von *Hašek*'s „Bravem Soldaten Schwejk“ bis zum Statistischen Jahrbuch für das Deutsche Reich 1935 wurde schon alles verwendet. Aber auch dieses System ist verwundbar; wird die Schlüsselquelle preisgegeben, öffnet sich ein ganzer Strom von Nachrichten auf einen Schlag.

Die kombinatorische Komplexität eines Verfahrens wird bestimmt durch die Anzahl der verfügbaren Schlüssel. Die Technik der Schlüssel ist individuell; sie wird bei den einzelnen Chiffrierverfahren besprochen werden.

2.6.2 Anknüpfend an 2.3.5 , sei $\mathbf{X}$ eine endlich erzeugte Blockchiffrierung,

$$\mathbf{X} = [\ \chi_{s_1}\ ,\ \chi_{s_2}\ ,\ \chi_{s_3}\ ,\ \dots\ ]\ , \qquad \text{wobei} \qquad \chi_{s_j} : p_j \mapsto c_j\ .$$

$(p_1, p_2, p_3, \dots)$, wo $p_j \in V^n$, bezeichnet dabei die Klartext-Zeichenfolge, $(c_1, c_2, c_3, \dots)$, wo $c_j \in W^m$, die zugehörige Geheimtext-Zeichenfolge.

k_j sei der Schlüssel, der χ_{s_j} bezeichnet, S_j sei ein Operator, der für $\chi_{s_j}(.)$ steht. Dann haben wir dreierlei Schreibweisen für die **Chiffriergleichung**

$$c_j = \chi_{s_j}(p_j) \qquad \text{oder} \qquad c_j = \mathbf{X}(p_j, k_j) \qquad \text{oder} \qquad c_j = p_j\ S_j\ .$$

Beachte, daß χ_i den i-ten Chiffrierschritt aus der Abzählung der Chiffrierschritte bezeichnet, während χ_{s_j} derjenige Chiffrierschritt ist, der im j-ten Schritt der Durchführung der Chiffrierung zur Anwendung kommt.

Ist, wie üblich, χ_{s_j} *injektiv und definal*, so existiert eine Umkehrung $\chi_{s_j}^{-1}$, für die (mit $\mathbf{Y} = [\ \chi_{s_1}^{-1}\ ,\ \chi_{s_2}^{-1}\ ,\ \chi_{s_3}^{-1}\ ,\ \dots\ ]$) gilt

$$p_j = \chi_{s_j}^{-1}(c_j) \qquad \text{oder} \qquad p_j = \mathbf{Y}(c_j, k_j) \qquad \text{oder} \qquad p_j = c_j\ S_j^{-1}\ .$$

Es ist also $\chi_{s_j}^{-1}(\chi_{s_j}(p_j)) = p_j$ und damit auch

$$\chi_{s_j}(\chi_{s_j}^{-1}(\chi_{s_j}(p_j))) = \chi_{s_j}(p_j)\ .$$

Ist χ_{s_j} auch *surjektiv und eindeutig*, also **eineindeutig**, so gilt sogar für *alle* $c_j \in W^m$

$$\chi_{s_j}(\chi_{s_j}^{-1}(c_j)) = c_j\ .$$

Beim **wechselseitigen Verkehr** zweier Partner kann dann der eine eine Folge von χ_{s_j} als Chiffrier- *und* Dechiffrierschritte, der andere die korrespondierende Folge von $\chi_{s_j}^{-1}$ als Chiffrier- *und* Dechiffrierschritte verwenden.

2.6.3 Sei wieder $\mathbf{X}$ eine endlich erzeugte Blockchiffrierung. Zwei Klartexte $(p'_1, p'_2, p'_3, \dots)$, $(p''_1, p''_2, p''_3, \dots)$ mit $p'_i = p''_i\, S$, wo S eine feste Substitution ist, heißen **isomorph**. Das gleiche gilt für zwei Geheimtexte $(c'_1, c'_2, c'_3, \dots)$, $(c''_1, c''_2, c''_3, \dots)$ mit $c'_i = c''_i\, T$, wo T eine feste Substitution ist. Nunmehr hat man für die Chiffrierschritte E'_i, E''_i:

$$\text{Ist } c'_i = p'_i E'_i \text{ und } c''_i = p''_i E''_i\ \text{, so ist } S\, E'_i = E''_i\, T\ .$$

Sind die Chiffrierungen umkehrbar, so werden isomorphe Klartexte in isomorphe Geheimtexte chiffriert und umgekehrt: Es ist dann

$$T = (E''_i)^{-1}\, S\, E'_i \quad \text{und} \quad S = E''_i\, T\, (E'_i)^{-1}\ .$$

Sind S und T umkehrbar, so können die Schlüssel ineinander umgerechnet werden:

$$E''_i = S\, E'_i\, T^{-1} \quad \text{und} \quad E'_i = S^{-1}\, E''_i\, T\ .$$

2.6.4 Ein Chiffrierschritt-System, bei dem jeder Chiffrierschritt und damit insbesondere das ihm zugeordnete Schlüsselzeichen eindeutig durch das Paar von Klartextzeichen und zugehörigem Geheimtextzeichen bestimmt ist, soll **Shannonsches Chiffrierschritt-System** und die zugehörige Chiffrierung **Shannonsche Chiffrierung** genannt werden. Viele der gebräuchlichen Chiffrierverfahren erfüllen diese **Shannon-Eigenschaft**.

Ein Chiffrierschritt-System, bei dem jeder Chiffrierschritt gleichzeitig auch Dechiffrierschritt ist und damit die Bestimmung des Schlüsselzeichens aus Klartextzeichen und Geheimtextzeichen symmetrisch ist, heißt **schlüsselsymmetrisch**. Jeder Chiffrierschritt ist damit **involutorisch** (s. auch 3.2.1).

3 Chiffrierschritte: Einfache Substitution

Unter den Chiffrierschritten betrachtet man vornehmlich die beiden großen Klassen Substitution und Transposition. Beide sind nur Spezialfälle des allgemeinen Chiffrierschritts $V^{(n)} \dashrightarrow W^{(m)}$. Wir werden zunächst verschiedene Arten der Substitution betrachten und uns erst im 6. Kapitel der Transposition zuwenden.

Für eine **einfache Substitution** (engl. *substitution*, frz. *substitution*), auch ‚Tauschverfahren' oder ‚Ersatzverfahren') sind alle Chiffrierschritte $\chi_i \in M$ monographisch, d.h. von der Gestalt

$$\chi_i : V^{(1)} \dashrightarrow W^{(m_i)} .$$

Aus M wird im monoalphabetischen Fall ein beliebiges χ_s ausgewählt und mit der Chiffrierung $X = [\chi_s\ ,\ \chi_s\ ,\ \chi_s\ ,\ ...]$ gearbeitet. Es genügt dann also, M einelementig zu nehmen.

Wir behandeln zuerst den Fall, daß für alle i $m_i = 1$ gilt.

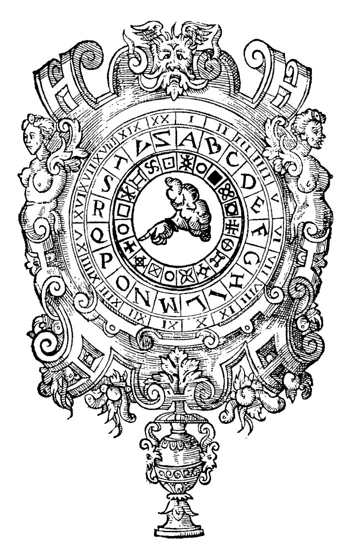


Abb. 23. Chiffrierscheibe von *Porta*, 1563

3.1 Fall $V^{(1)} \dashrightarrow W$ (unipartite einfache Substitutionen)

Im Falle $V^{(1)} \dashrightarrow W$ handelt es sich um eine **unipartite einfache Substitution**, auch **einfache Substitution** schlechthin genannt.

3.1.1 $V \longrightarrow W$, Chiffrierung ohne Homophone und ohne Blender.

Dieser Fall ist uralt. Für W wird gern ein Alphabet seltsam geformter, unüblicher Zeichen verwendet: in Thailand, Persien, im koptischen Äthiopien

und anderswo. Solche Zeichen verwendet *Giovanni Battista Porta* (*Giambattista Della Porta*, 1535–1615) auf seiner Chiffrierscheibe (Abb. 23). Auch *Karl der Große* soll solche Zeichen benutzt haben (Abb. 24) und, nach Bernhard Bischoff, die hl. Hildegard von Bingen (1098–1179), die vielseitige Gelehrte.

a b c d e f g h i k l m n o p q r ſ t u x y z

Abb. 24. Geheimzeichen *Karls des Großen*

Die Freimaurerchiffre (engl. auch *pigpen cipher*) fällt hierunter; in ihrer modernen Form lautet sie

a b c d e f g h i j k l m n o p q r s t u v w x y z

Sie kann memoriert werden durch die Schemata

a	b	c	(ohne
d	e	f	Punkt)
g	h	i	

j	k	l	(mit
m	n	o	Punkt)
p	q	r	

s, t, u, v (ohne Punkt) — w, x, y, z (mit Punkt)

Noch 1728 wurde am Zarenhof (neben Nomenklatoren) eine heteromorphe Substitution $V \longrightarrow W$ mit einem bizarren Geheimzeichenvorrat verwendet.

Literarisch berühmt wurde eine heterogene Substitution mit gewöhnlichen Lettern durch *Edgar Allan Poes* Erzählung “The Gold-Bug” (s. 15.10.1).

Hierunter fällt auch die Kaufmanns-Chiffre für Preisauszeichnung und Datumskennung, eine Abbildung $Z_{10} \longrightarrow Z_{26}$, die durch ein **Kennwort** (engl. *password*) oder einen **Kennsatz** erzeugt wird (‘key-phrase’ cipher); etwa mit dem Kennwort MILCHPROBE

1	2	3	4	5	6	7	8	9	0
M	I	L	C	H	P	R	O	B	E

Dieser Chiffrierschritt wurde bei der Kennzeichnung des Verpackungsdatums von Butter über Jahre hinweg gebraucht. Ebenso wurde in ENIGMA-Chiffrierungen der Marine manchmal Ziffern durch Buchstaben wiedergegeben:

1	2	3	4	5	6	7	8	9	0
q	w	e	r	t	z	u	i	o	p

3.1.2 $V^{(1)} \dashrightarrow W$, Chiffrierung mit Homophonen und Blendern.

Homophone finden sich schon in arabischen Quellen, etwa bei *al-Qalqashandi* 1412 und in einer Chiffrierung, die das Herzogtum *Mantua* 1401 für einen Briefwechsel mit *Simeone de Crema* benutzte. Die Vokale – bezeichnenderweise also die häufiger vorkommenden Zeichen – besaßen Homophone, ein erstes Anzeichen von Überlegungen zur Nivellierung der Häufigkeiten. Dazu wurde W durch Ziffern erweitert. Die Einführung von Homophonen legt praktisch die Einführung von Blendern nahe: Sonst erkennt man zu leicht Homophone am umgebenden gleichbleibenden Wortmuster häufiger Wörter.

Ein bis heute benutztes Verfahren mit Homophonen ist die **Buchchiffre**: In einem (beim Sender und beim Empfänger in identischen Kopien vorhandenen) unverfänglichen Buch wird ein Buchstabe nach dem anderen aufgesucht, die dazugehörigen Lagen werden etwa durch Angabe von Seite, Zeile und Position chiffriert: Wird als Buch das vorliegende (3. Auflage) gewählt, so kann m u m m e l durch 3-7-1, 5-6-5, 6-12-6, 4-5-3, 7-8-3, 5-2-11 chiffriert werden.

3.2 Spezialfall $V \leftarrow\!\!\!\rightarrow V$ (Permutationen)

Im eineindeutigen Falle $V \leftarrow\!\!\!\rightarrow W$ unter den Beispielen in 3.1.1 spricht man von einem **umgeordneten Alphabet** W (engl. *mixed alphabet*, frz. *alphabet désordonné, alphabet incohérent*) von N Klartextzeichen, das einem **Standard-Alphabet** V von N Geheimtextzeichen **gegenübersteht**.

Zur Definition einer Substitution genügt es, irgendwie die Paarungen von Klartextzeichen und Geheimtextzeichen aufzulisten, etwa für $V = Z_{26}$ und $W = Z_{26}$ (Verwendung von Kleinbuchstaben und Kapitälchen, vgl. 2.5.6):

u d c b m a v g k s t n w z e i h f q l j r o p x y
H E W A S R I G T O U D C L N M F Y V B P K J Q Z X

Für den Chiffrierer ist es natürlich bequemer, die Klartextzeichen in einer geläufigen Weise, also nach einem Standard-Alphabet, geordnet zu haben:

a b c d e f g h i j k l m n o p q r s t u v w x y z
R A W E N Y G F M P T B S D J Q V K O U H I C Z X L

In der Mathematik ist diese ‚Substitutionsschreibweise' üblich. Für den Dechiffrierer ist es aber besser, die Geheimtextzeichen nach einem Standard-Alphabet anzuordnen:

b l w n d h g u v o r z i e s j p a m k t q c y f x
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Eine neue Situation liegt vor im endomorphen Fall $V \doteq W$. Speziell die eineindeutige Substitution $V \leftarrow\!\!\!\rightarrow V$ heißt dann **Permutation** von V. Permutationen sind in elektrischen Realisierungen durch Vertauschen von Leitungen in Leitungsbündeln erzielbar.

Für Permutationen ist in der Mathematik neben der Substitutionsschreibweise auch die ‚Zyklenschreibweise' gebräuchlich, in unserem Beispiel

(a r k t u h f y x z l b) (c w) (d e n) (g) (i m s o j p q v) .

Dabei muß die unterschiedliche Schreibung mit Kleinbuchstaben und Kapitälchen aufgegeben werden. Für den Chiffrierschritt geht man in dem Zyklus, in dem man den Klartextbuchstaben gefunden hat, zum (zyklisch) nachfolgenden Buchstaben, für den Dechiffrierschritt zum vorausgehenden. Einerzyklen werden oft nicht notiert – wir werden dem meist nicht folgen.

3.2.1 Die ältesten Quellen (wenn man von Ägypten absieht – wir werden unter ‚Code' darauf zurückkommen) zeigen eine **involutorische** (engl. oft *self-reciprocal*, *reciprocal*, frz. *réciproque*) Abbildung von V in sich, und zwar in Indien: Im *Kāma-sūtra* des *Vātsyāyana* wird Geheimschrift als eine

der 64 Künste erwähnt, als *Mūladevīya* wird bezeichnet die Vorschrift (die übrigen Buchstaben bleiben invariant):

$$V \overset{2}{\longleftrightarrow} V \ : \updownarrow \begin{array}{l} \text{a kh gh c t ñ n r l y} \\ \text{k g n ṭ p ṇ m ṣ s ś} \end{array} \ .$$

Ein anderes Beispiel einer allgemeinen involutorischen Abbildung benutzte 1780 die amerikanische Studentenverbindung Phi Beta Kappa ($V = Z_{26}$):

$$V \overset{2}{\longleftrightarrow} V \ : \updownarrow \begin{array}{l} \text{a b c d e f g h i j m n s} \\ \text{u t y l z o k p w v q r x} \end{array} \ .$$

Im hebräischen Alten Testament wurde eine furchenwendige Substitution verwendet (‚Atbasch', **revertiertes Alphabet**, engl. *inverse alphabet*, frz. *alphabet inversé*), die im lateinischen Alphabet ($V = Z_{20}$) so lauten würde:

$$V \overset{2}{\longleftrightarrow} V \ : \updownarrow \begin{array}{l} \text{a b c d e f g h i l} \\ \text{z v t s r q p o n m} \end{array} \ .$$

Dem steht gegenüber eine involutorische Abbildung mit einem **komplementären** (Standard-)Alphabet (*Eyraud*: *alphabet complémentaire*), s. 5.6 :[1]

$$V \overset{2}{\longleftrightarrow} V \ : \updownarrow \begin{array}{l} \text{a b c d e f g h i l m} \\ \text{a z v t s r q p o n m} \end{array} \ .$$

Naheliegend ist auch eine involutorische Abbildung mit einem **verschobenen Alphabet** wie das hebräische ‚Albam', von den *Argentis* 1589 gebraucht:

$$V \overset{2}{\longleftrightarrow} V \ : \updownarrow \begin{array}{l} \text{a b c d e f g h i l} \\ \text{m n o p q r s t v z} \end{array}$$

oder (*Porta* 1563, s. 7.4.4, Abb. 53, mit $V = Z_{22}$)

$$V \overset{2}{\longleftrightarrow} V \ : \updownarrow \begin{array}{l} \text{a b c d e f g h i l m} \\ \text{n o p q r s t v x y z} \end{array} \ .$$

Den allgemeinen furchenwendigen Fall mit einem Kennwort zeigt ($V = Z_{26}$)

$$V \overset{2}{\longleftrightarrow} V \ : \updownarrow \begin{array}{l} \text{a n g e r s b c d f h i j} \\ \text{z y x w v u t q p o m l k} \end{array} \ .$$

Der Vorteil involutorischer Abbildungen liegt generell in der kompakten Schreibweise und dem von manchen Leuten für wichtig gehaltenen Umstand, daß Chiffrierschritt und Dechiffrierschritt identisch sind.

In der Zyklenschreibweise der Permutationen würden wir die letzten fünf Beispiele schreiben (mit alphabetisch geordneten Zyklenanfängen)

(a,z) (b,v) (c,t) (d,s) (e,r) (f,q) (g,p) (h,o) (i,n) (l,m)
(a) (b,z) (c,v) (d,t) (e,s) (f,r) (g,q) (h,p) (i,o) (l,n) (m)
(a,m) (b,n) (c,o) (d,p) (e,q) (f,r) (g,s) (h,t) (i,v) (l,z)
(a,n) (b,o) (c,p) (d,q) (e,r) (f,s) (g,t) (h,v) (i,x) (l,y) (m,z)
(a,z) (b,t) (c,q) (d,p) (e,w) (f,o) (g,x) (h,m) (i,l) (j,k) (n,y) (r,v) (s,u)

Echt involutorisch ist eine Abbildung, die keine Einerzyklen, also (wie oben vorwiegend) nur Zweierzyklen (engl. *swaps*) hat. Gegen sie gibt es besondere Angriffsmöglichkeiten (s. 14.1), die schon entfallen, wenn *einige* der Zyklen einer involutorischen Permutation Einerzyklen (engl. *females*) sind.

---

[1] Es handelt sich aber um keine echte Involution: a und m gehen in sich über.

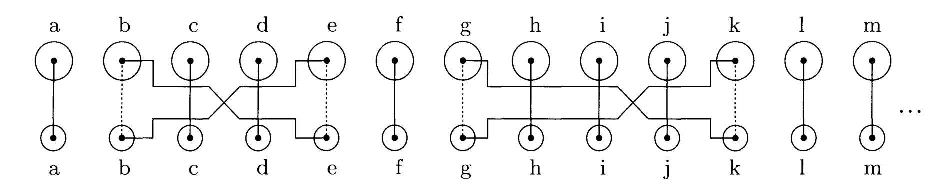


Abb. 25. Involutorische Substitution mittels Doppelsteckerpaar und Schaltklinken

Im Fall eines binären Alphabets ($V = Z_2$) ist die einzige nichttriviale Permutation involutorisch:

$$V \overset{2}{\longleftrightarrow} V \ : \updownarrow \begin{matrix}\mathbf{O}\\ \mathbf{L}\end{matrix} \quad .$$

3.2.2 Involutionen sind in elektrischen Realisierungen durch Vertauschung von Leitungspaaren erzielbar, technisch einfach durch Doppelstecker und Schaltklinken (Abb. 25). Solche Involutionen werden im Steckerbrett der ENIGMA verwendet. Die Anzahl $d(k, N)$ der Involutionen hängt von N und von der Anzahl k der benutzten (Doppel-)Steckerpaare ab: es ist

$$d(k,N) = \frac{N!}{2^k \cdot (N-2k)! \cdot k!} = \binom{N}{2k} \cdot \frac{(2k)!}{2^k k!} = \binom{N}{2k} \cdot (2k-1)!! \ .$$

Echte Involutionen verlangen, daß $N = 2\nu$ gerade ist. Die Anzahl aller echten Involutionen ist dann (mit einem relativen Fehler $< 10^{-3}$ für $N \geq 6$)

$$d(\tfrac{N}{2}, N) = (N-1)!! \ = \ (N-1)\cdot(N-3)\cdot \ \ldots \ \cdot 5 \cdot 3 \cdot 1 = \tfrac{(2\nu)!}{\nu! 2^\nu} \ \approx \ \frac{\sqrt{(2\nu)!}}{\sqrt[4]{\pi \cdot (\nu + \frac{1}{4})}} \ .$$

Die Abschätzung liefert eine recht gute obere Schranke für $(N-1)!!$.

Bei festem N wird jedoch $d(k, N)$ bereits maximal für $k \approx \nu - \sqrt{(\nu+1)/2}$:
$d(5,26) \approx 5.02 \cdot 10^9$, $d(6,26) \approx 1.00 \cdot 10^{11}$, $d(7,26) \approx 1.31 \cdot 10^{12}$,
$d(8,26) \approx 1.08 \cdot 10^{13}$, $d(9,26) \approx 5.38 \cdot 10^{13}$, $d(10,26) \approx 1.51 \cdot 10^{14}$,
$d(11,26) \approx 2.06 \cdot 10^{14}$, $d(12,26) \approx 1.03 \cdot 10^{14}$, $d(13,26) \approx 7.91 \cdot 10^{12}$

und $d(3,10) = 3150$, $d(4,10) = 4725$, $d(5,10) = 945$.

Die ENIGMA I der Reichswehr von 1930 verwendete ursprünglich 6 Steckerpaare, die Wehrmachts-ENIGMA ab 1.10.1936 5–8 Steckerpaare, ab 1.1.1939 7–10 Steckerpaare, ab 19.8.1939 10 Steckerpaare.

3.2.3 Eine kompakte Notation erlaubt auch die **voll zyklische Permutation** mit genau einem Zyklus, die von der Ordnung N ist:
etwa mit $N = 20$ der **Zyklus des Standard-Alphabets** Z_{20}

$$V \overset{N}{\longleftrightarrow} V \ : (\text{a b c d} \ldots \text{t v x})$$

oder dessen dritte Potenz[2]

$$V \overset{N}{\longleftrightarrow} V \ : (\text{a d g l o r v b e h m p s x c f i n q t}) \ ;$$

[2] Die zweite Potenz ist jedoch nur von der Ordnung 10, und die zehnte Potenz ist nur noch von der Ordnung 2: es ist eine der oben betrachteten involutorischen Abbildungen. Die $(N-1)$-te Potenz ist invers zur 1. Potenz und liefert den Dechiffrierschritt.

in Substitutionsschreibweise[3]

a b c d ... t v x		a b c d ... t v x
B C D E ... V X A	bzw.	D E F G ... A B C .

Letzteren Chiffrierschritt hat *Julius Caesar* (nach *Suetonius*) benutzt, im Alphabet drei Buchstaben weiterzählend. Sein Nachfolger *Augustus*, *Caesar* in mancher Hinsicht unterlegen, benutzte die erstere Substitution (vielleicht konnte er nicht bis drei zählen; nach *Suetonius* ersetzte er auch x durch AA). Jede Potenz des Zyklus des Standard-Alphabets liefert ein CAESAR-Alphabet. Wir werden darauf im 5. Kapitel (CAESAR-Addition) zurückkommen.

Eine monoalphabetische Substitution mit einem CAESAR-Chiffrierschritt wurde 1915 in der russischen Armee eingeführt, nachdem sich herausgestellt hatte, daß man den Stäben etwas Komplizierteres nicht zumuten konnte. Für *Ludwig Deubner* und *Hermann Pokorny*, die Chefs der Entzifferungsdienste, war das ein Leckerbissen (ein ‚gefundenes Fressen' bzw. ein ‚gmahtes Wiesl').

Ihrer Natur nach genügen eine Spur auf einer Scheibe, der Rand einer Münze oder ein zum Ring geschlossener Streifen zur Darstellung eines vollen Zyklus. Solche Hilfsmittel wurden weithin gebraucht, in besonderer Weise (s. 7.5) benutzten sie *Jefferson* (um 1795) und *Bazeries* (1891). Die q-te Potenz erhält man durch Weiterzählen im Zyklus um jeweils q Zeichen (s. 3.2.8).

3.2.4 Auch für nicht-involutorisches und nicht-zyklisches $V \rightarrowtail\!\!\twoheadrightarrow V$ wird der allgemeinste Fall eines **permutierten Alphabets** (engl. *mixed alphabet*, frz. *alphabet désordonné*) normalerweise in Substitutionsschreibweise notiert:

$V \rightarrowtail\!\!\twoheadrightarrow V$: a b c d e f g h i j k l m n o p q r s t u v w x y z
S E C U R I T Y A B D F G H J K L M N O P Q V W X Z

Zyklenschreibweise ergibt

$V \rightarrowtail\!\!\twoheadrightarrow V$: (a s n h y x w v q l f i) (b e r m g t o j) (c) (d u p k) (z) ,

einen Zwölfer-, einen Achter-, einen Viererzyklus nebst zwei Einerzyklen.

3.2.4.1 Weitere permutierte Alphabete bekommt man durch zyklische *Verschiebung* einer der beiden Zeilen in der Substitutionsschreibweise (**verschobene permutierte Alphabete**, frz. *alphabets désordonnés parallèles*)

$V \rightarrowtail\!\!\twoheadrightarrow V$: a b c d e f g h i j k l m n o p q r s t u v w x y z
E C U R I T Y A B D F G H J K L M N O P Q V W X Z S

$V \rightarrowtail\!\!\twoheadrightarrow V$: a b c d e f g h i j k l m n o p q r s t u v w x y z
C U R I T Y A B D F G H J K L M N O P Q V W X Z S E

in Zyklenschreibweise

$V \rightarrowtail\!\!\twoheadrightarrow V$: (a e i b c u q m h) (d r n j) (f t p l g y z s o k) (v) (w) (x) ,

$V \rightarrowtail\!\!\twoheadrightarrow V$: (a c r o l h b u v w x z e t q n k g) (f y s p m j) (d i) .

---

[3] Man spricht auch hier — sich auf die zweite Zeile des Substitutionsausdrucks beziehend — von Standardalphabeten (engl. *standard alphabet*, frz. *alphabet ordonné*) und entsprechend von einer Standardalphabet-Chiffrierung (engl. *standard alphabet cipher*).

3.2.4.2 Durch *Potenzierung* erhält man die **potenzierten permutierten Alphabete**, etwa aus der Substitution SECURITY... von oben mit einer zweiten Potenz

$V \longleftrightarrow V$: (a n y w q f) (b r g o) (c) (d p) (e m t j) (h x v l i s) (k u) (z),

wobei alle Zyklen gerader Länge halbiert werden; in Substitutionsschreibweise

$V \longleftrightarrow V$:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
N	R	C	P	M	A	O	X	S	E	U	I	T	Y	B	D	F	G	H	J	K	L	Q	V	W	Z

Potenzierung einerseits, Verschiebung andererseits liefern i.a. nicht das gleiche; es handelt sich um zwei grundverschiedene Verfahren zur Erzielung einer **Familie** von bis zu N **begleitenden Alphabeten** (s. 7.1, 7.2).

3.2.5 Die obigen Beispiele lassen bereits die Konstruktion der einfachen endomorphen Substitution $V \longleftrightarrow V$ mittels eines „Schlüssels“ erkennen: Eine klassische Methode benutzt *memorierbare* **Kennwörter** oder **Kennsätze** (‚Merkwort‘, ‚Merkvers‘, ‚Losung‘, engl. *password, mnemonic key*), schreibt deren Buchstaben ohne Wiederholung an und fügt sodann die noch nicht verwendeten Buchstaben in Alphabetreihenfolge an. Für den Fall der so definierten Substitution geht die Methode auf die *Argenti*s, um 1580, zurück. Sie gehört bis heute zum kryptologischen Standard.[4]

Diese Konstruktion ist aber anfällig. Zu leicht kann ein fehlender Teil des Kennworts erraten werden (immerhin treffen die häufigen Vokale e und a immer auf einen Kennwort-Buchstaben, wenn das Kennwort wenigstens die Länge 5 hat). Zumindest sollte das Kennwort keine ‚Auffüllung‘ erfordern. Raffiniertere Methoden benutzen eine Umstellung der Sequenz, beispielsweise indem diese erst zeilenweise geschrieben und dann spaltenweise abgelesen wird[5] (Verfahren von *Wheatstone*, 1854).

S	E	C	U	R	I	T	Y
A	B	D	F	G	H	J	K
L	M	N	O	P	Q	V	W
X	Z						

a	e	i	l	o	r	u	x
b	f	j	m	p	s	v	y
c	g	k	n	q	t	w	z
d	h						

Damit ergibt sich das Alphabet

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
S	A	L	X	E	B	M	Z	C	D	N	U	F	O	R	G	P	I	H	Q	T	J	V	Y	K	W

bzw. in Zyklenschreibweise mit dem Einerzyklus (e)

(a s h z w v j d x y k n o r i c l u t q p g m f b) (e)

Ein weiteres Verfahren füllt auch noch die Spalten der Klartextseite in der Alphabetordnung der Buchstaben des Kennworts, also in der Reihenfolge

dritte, zweite, sechste, fünfte, erste, siebte, vierte, achte Spalte

---

[4] Läßt man Wiederholungen zu, so kommt man zu Polyphonen, etwa (s. 2.4)

a	b	c	d	e	f	g	h	i	j	l	m	n	o	p	q	r	s	t	u	v	x	y	z	
L	E	G	O	U	V	E	R	N	E	M	E	N	T	P	R	O	V	I	S	O	I	R	E	.

und verkürzt den Geheimtextzeichenvorrat (hier auf 14 Zeichen, $\{b, g, j, m, z\} \mapsto E$) .

[5] Solch eine Umstellung wird in 6.2 methodisch als ein Chiffrierverfahren (Transposition) behandelt werden.

mit dem Ergebnis

S	E	C	U	R	I	T	Y	n	d	a	u	k	h	r	x
A	B	D	F	G	H	J	K	o	e	b	v	l	i	s	y
L	M	N	O	P	Q	V	W	p	f	c	w	m	j	t	z
X	Z							q	g						

Damit erhält man das Alphabet

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C	D	N	E	B	M	Z	I	H	Q	R	G	P	S	A	L	X	T	J	V	U	F	O	Y	K	W

bzw. in Zyklenschreibweise

(a c n s j q x y k r t v f m p l g z w o) (b d e) (h i) (u) .

Die geschilderte Methode kann auch für die Gewinnung von Zyklen benutzt werden. Der Kennsatz ≪*évitez les courants d'air*≫ („vermeidet Zugluft“ , *Bazeries*, 7.4.3) liefert

$V \overset{N}{\leftarrow\!\!\!\rightarrow} V$: (e v i t z l s c o u r a n d b f g h j k m p q x y)

3.2.6 Nachfolgende Tabelle gibt für $N = 26$, für $N = 10$ und für $N = 2$ einen Überblick über die Anzahl der verfügbaren Alphabete $V \leftarrow\!\!\!\rightarrow V$:

Anzahl der Permutationen	$Z(N)$	$Z(26)$	$Z(10)$	$Z(2)$
alle	$N!$	$4.03 \cdot 10^{26}$	3628800	2
voll zyklische	$(N-1)!$	$1.55 \cdot 10^{25}$	362880	1
involutorische insgesamt	$\approx N\cdot(N!)^{\frac{1}{2}}$	$5.33 \cdot 10^{14}$	9496	2
echt involutorische	$\approx (N!)^{\frac{1}{2}}$	$7.91 \cdot 10^{12}$	945	1
aus sinnvollen Kennwörtern (‚Merkwörtern‘) gewonnene		10^4 ... 10^6		

3.2.7 Zur Mechanisierung einer Substitution kann man die feste Gegenüberstellung der Klartext- und der Geheimtextzeichen, wie sie sich in der Substitutionsschreibweise findet, auch auf *einem* Lineal (engl. *strip*) oder *einer* Walze (engl. *cylinder*) unterbringen und durch zwei Fenster die beiden jeweils zusammengehörigen Zeichen sichtbar werden lassen. Diese Fenster können auch so angeordnet werden, daß der Meister nur das Klartextfenster, der Schreiber nur das Geheimtextfenster sieht und damit den Sinn der Nachricht nicht versteht (s. 7.5.2, Maschine von *Gripenstierna*, Abb. 54). Eine Auswahl aus N begleitenden *verschobenen* Alphabeten erhält man, wenn man etwa das Geheimtextfenster verschiebbar macht.

Eine andere Möglichkeit besteht darin, Klar- und Geheimtextalphabet gegeneinander verschiebbar zu machen durch Verwendung zweier gegeneinander verdrehbarer **Scheiben** (Abb. 26) oder zweier gegeneinander verschiebbarer **Lineale** (Abb. 27). Im letzteren Fall ist es erforderlich, daß eines der Alphabete wiederholt wird (**Duplikation**).

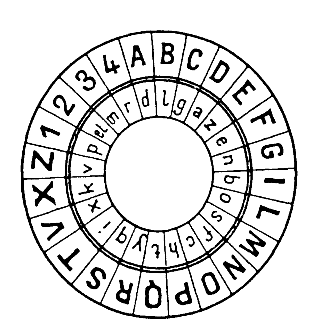


Abb. 26.
Chiffrierscheibe von
Leon Battista Alberti
(nach *Lange-Soudart* 1935)

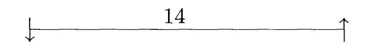
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	...
						S	E	C	U	R	I	T	Y	A	B	D	F	G	H	J	K	L	M	N	O	P	Q	V	W	X	Z								

Abb. 27. Chiffrierschieber mit dupliziertem Klartextalphabet

Chiffrierscheiben (engl. *cipher disk*, frz. *cadran*) als mechanische Hilfsmittel für allgemeine Substitution mit verschobenen permutierten Alphabeten wurden schon 1466 von *Leon Battista Alberti* beschrieben[6], s. a. Farbtafel B. **Chiffrierschieber** (engl. *cipher slide*, frz. *réglette à chiffrer*) wurden schon im elisabethanischen England, um 1600, verwendet. Im 19. Jh. wurden sie Saint-Cyr-Schieber, nach der gleichnamigen französischen Kriegsschule, genannt. Dem selben Zweck dienen **Chiffrierstäbchen** (frz. *bâtons*, engl. *rods*).

3.2.8 Zur Mechanisierung einer einzigen *voll zyklischen* Permutation kann man auch von der Zyklenschreibweise ausgehen. Man bringt den Zyklus auf einem Lineal unter (das erste Zeichen muß wiederholt werden) oder auf einer Walze und sieht zwei unmittelbar benachbarte Fenster für das Ablesen der Klar- und der Geheimtextzeichen vor.

Eine Auswahl aus N begleitenden **potenzierten** Alphabeten erhält man wieder, wenn man den Abstand zwischen den beiden Fenstern veränderlich macht. Im Falle des Lineals muß das ganze Alphabet wiederholt werden. Die q-te Potenz der vollen zyklischen Permutation erhält man, wenn die Fenster einen Abstand von q Zeichen haben (Abb. 28 für $q = 14$).



S	E	C	U	R	I	T	Y	A	B	D	F	G	H	J	K	L	M	N	O	P	Q	V	W	X	Z	S	E	C	U	R	I	T	Y	A	B	D	F	G	...

Abb. 28. Chiffrierlineal mit Fenstern für Potenzen eines Alphabets

---

6 Bei *Alberti* sind möglicherweise, abweichend vom modernen Gebrauch, Großbuchstaben Klartext, Kleinbuchstaben Geheimtext. Das Zeichen *et* steht vermutlich für das Symbol & . Die Anfangseinstellung der Scheibe erfolgt durch Gegenüberstellung eines **Schlüsselbuchstabens**, etwa D, zu einem festen Buchstaben, etwa /a/ .

3.3 Fall $V^{(1)} \dashrightarrow W^m$ (multipartite einfache Substitutionen)

3.3.1 $m = 2$, bipartite einfache Substitutionen $V^{(1)} \dashrightarrow W^2$.

Es handelt sich um Substitutionen *durch* Bigramme. Mit $|W| = 5$ liegt hier ebenfalls ein altes Verfahren einer Quinärchiffrierung vor, das schon *Polybius* gekannt haben soll. Z_{25} wird in ein 5×5-Quadrat eingeschrieben:

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

oder

	1	2	3	4	5
1	a	f	l	q	v
2	b	g	m	r	w
3	c	h	n	s	x
4	d	i	o	t	y
5	e	k	p	u	z

Nach der Vorschrift rechts ergibt sich für das Textsemagramm

3 3 5 1 5 1 4 1 2 3 4 3 3 3 5 1 4 5 1 2 4 3 2 4 1 1 3 4 3 4 1 1 3 4 3 4 4 2 3 3 1 1 4 4 4 2 4 3 3 3

von 1.1, Abb. 5 der Klartext

n e e d m o n e y f o r a s s a s s i n a t i o n .

Diese spezielle Chiffrierung $Z_{25} \longrightarrow Z_5 \times Z_5$ hat sich als internationaler Klopf-Code bis heute in Haftanstalten gehalten. Die normale Übertragungsgeschwindigkeit beträgt 10–15 Wörter pro Minute. Im Zarenreich wurde ein solcher Klopf-Code (mit einem 6×6-Quadrat) verwendet und gelangte mit russischen Anarchisten nach Westeuropa (‚Anarchistenchiffre'), wurde auch steganographisch benutzt (vgl. 1.2). Über den Gebrauch in der Sowjetunion berichteten *Arthur Koestler* in ‚Sonnenfinsternis' (Volkskommissar *Rubaschow* an den Häftling in Zelle 402) und *Alexander Solschenizyn* in ‚Der Archipel GULAG'.

Im allgemeinen arbeitet man mit einem Kennwort, das zeilenweise ins Quadrat eingeschrieben wird und ergänzt dieses dann. Der *Graf Mirabeau*, ein französischer Revolutionär des 18. Jahrhunderts, verwendete dieses Verfahren in Briefen an die *Marquise de Monnier* — er schloß allerdings ein tomographisches Verfahren (s. 9.5.1) an und nahm 6 7 8 9 0 als Blender hinzu.

Mit $|W| = 6$ und Quadraten wie

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	l	0	j	d
G	5	s	i	y	h	u
V	p	1	v	b	6	r
X	e	q	7	t	2	g

arbeitete das ADFGVX-System, das unter *Ludendorff* 1918 an der Westfront im Funkverkehr eingesetzt wurde (für das Geheimalphabet Z_6 vgl. 2.5.2).

Auch rechteckige Anordnungen werden benutzt. So findet man schon bei *Giovanni Batista Argenti* um 1580 das Schema mit $W = Z_{10}$ (denär)

	0	1	2	3	4	5	6	7	8	9
1	p	i	e	t	r	o	a	b	c	d
2	f	g	h	l	m	n	q	s	u	z

und damit die erste Verwendung eines Kennworts überhaupt. Auch Homophone können so leicht eingeführt werden:

	1	2	3	4	5	6	7	8	9
9, 6, 3	a	b	c	d	e	f	g	h	i
8, 5, 2	j	k	l	m	n	o	p	q	r
7, 4, 1	s	t	u	v	w	x	y	z	

.

Besser ist es, bei den Homophonen auf die Häufigkeit zu achten. Ausgehend von der Häufigkeitsreihenfolge des Englischen e t a o n i r s h (zusammen etwa 70 %) ergibt sich als eine gute Annäherung an eine **Nivellierung**

	1	2	3	4	5	6	7	8	9	
4,5,6,7,8,9,0	e	t	a	o	n	i	r	s	h	71.09 %
2,3	b	c	d	f	g	j	k	l	m	19.46 %
1	p	q	u	v	w	x	y	z		9.45 %

.

In den beiden letzten Beispielen kann 0 als Blender dienen.[7] Eine andere Methode benutzt ein 4-buchstabiges Kennwort und setzt damit den Beginn der Zyklen (**00**..24), (**25**..49), (**50**..74), (**75**..99) fest (mit $V = Z_{25}$) für eine homophonische Chiffre, etwa mit dem Kennwort *KILO*:

	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
K	16	17	18	19	20	21	22	23	24	**00**	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
I	42	43	44	45	46	47	48	49	**25**	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
L	65	66	67	68	69	70	71	72	73	74	**50**	51	52	53	54	55	56	57	58	59	60	61	62	63	64
O	87	88	89	90	91	92	93	94	95	96	97	98	99	**75**	76	77	78	79	80	81	82	83	84	85	86

Eine nicht homophonische bipartite Chiffre über Z_{10} benutzte schon 1786 der schwedische Baron *Fridric Gripenstierna* – möglicherweise auf *Christopher Polheim* zurückgehend. Eine spaßige Form einer bipartiten Chiffre mit Homophonen wurde zwischen Brig. Gen. *Leslie R. Groves* und Lt. Col. *Peer da Silva* in Los Alamos verabredet (Abb. 29), um bei Telefongesprächen besondere Namen und Bezeichnungen geheimhalten zu können. Das raffinierte daran ist, daß man die Buchstaben suchen muß und damit Homophone womöglich mehr zufällig auswählt als sonst, wo die Chiffrierer meist voreingenommen (engl. *biased*) vorgehen.

3.3.2 $m = 3$, tripartite einfache Substitutionen $V^{(1)} \dashrightarrow W^3$

Es handelt sich um Substitutionen *durch* Trigramme. Mit $|W| = 3$ schlägt schon *Trithemius* in der *Polygraphiae* von 1518 für steganographische Zwecke eine solche Abbildung vor, $W = \{1,\ 2,\ 3\}$, $|W^3| = 27$. Ternärchiffrierung wie diese wird selten verwandt.

---

[7] Null, ursprünglich *nulla ziffra*, wird immer noch nicht überall ernst genommen.

1	2	3	4	5	6	7	8	9	0	
I	P	I		O	U	O		P	N	1
W	E	U	T	E	K		L	O		2
E	U	G	N	B	T	N		S	T	3
T	A	Z	M	D		I	O	E		4
S	V	T	J		E		Y		H	5
N	A	O	L	N	S	U	G	O	E	6
	C	B	A	F	R	S		I	R	7
I	C	W	Y	R	U	A	M		N	8
M	V	T		H	P	D	I	X	Q	9
L	S	R	E	T	D	E	A	H	E	0

Abb. 29. Bipartite Chiffre, in Los Alamos 1944 bei Telefongesprächen verwendet

3.3.3 $m = 5$, quinpartite einfache Substitutionen $V^{(1)} \dashrightarrow W^5$

Es handelt sich um Substitutionen *durch* Pentagramme. Mit $|W| = 2$ wird quinpartite Substitution schon von *Francis Bacon* zu steganographischen Zwecken (vgl. 1.2) verwendet. Quinpartite Binärchiffrierung ($|W^5| = 32$) findet ihre Wiederauferstehung in der Chiffriermaschine von *Vernam* 1918 (s. 8.3.2) und im Siemens-Geheimschreiber (s. 9.1.3).

3.3.4 $m = 8$, octopartite einfache Substitutionen $V^{(1)} \dashrightarrow W^8$

Mit $|W| = 2$ (binärer EBCDIC-Code oder gesicherter ASCII-Code) wird diese Substitution *durch* Bytes in den modernen Rechenanlagen verwendet.

3.4 Der allgemeine Fall $V^{(1)} \dashrightarrow W^{(m)}$, Spreizen

Der allgemeine Fall $V^{(1)} \dashrightarrow W^{(m)}$ lädt geradezu zur Verwendung von Blendern und Homophonen ein.

Simeone di Crema in Mantua (1401) benutzte (mit $m = 1$) lediglich Homophone. Mit $m = 2$ wird dann neben Homophonen und Blendern noch ein wichtiger Gedanke ins Spiel gebracht: Das ‚Spreizen' des Alphabets (engl. *straddling*), die Abbildung von V in $W^1 \cup W^2$. Auf *Matteo Argenti* geht eine nach 1590 am päpstlichen Hof verwendete Chiffre zurück, die Homophone, Blender und Spreizen zeigt. Für ein um die Wörter et con non che erweitertes Alphabet Z_{24} gibt er (mit Blendern 5, 7) die Spreizung an als

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	v	z	et	con	non	che	ε
1	86	02	20	62	22	06	60	3	24	26	84	9	66	68	28	42	80	04	88	08	64	00	44	5
				82													40							7

3.4.1 Gespreizte Chiffrierung unterliegt der Einschränkung, daß die dadurch induzierte Chiffrierung injektiv ausfallen muß – dies bedeutet, daß die **Wortfuge** zwischen den ein- und zweibuchstabigen Chiffren eindeutig rekonstruierbar sein muß. Wie schon in 2.4 gesagt, kannte *Giovanni Batista Argenti* und sein Neffe *Matteo* bewußt oder unbewußt diesen Sachverhalt,

jedenfalls genügten ihre Chiffren dieser Bedingung. Auch für die noch zu besprechenden gespreizten Chiffren gilt dies: W wird zerlegt in

Zeichen für einelementige Chiffren: $W' = \{1, 3, 5, 7, 9\}$ und
Zeichen, mit denen zweielementige Chiffren beginnen: $W'' = \{0, 2, 4, 6, 8\}$.

Die *Argentis* schrieben vernünftigerweise des weiteren vor, nach dem q das u zu unterlassen sowie Buchstabenverdopplungen zu unterdrücken. Es unterlief ihnen aber auch der Fehler, die zweiten Elemente der zweielementigen Chiffren auf W'' zu beschränken: Dies legt die Spreizung offen.

Gespreizt sind insbesondere die sogenannten **Spionage-Chiffren**, die der NKWD (*Narodni Komisariat Wnustrennich Del*) und seine Nachfolger verwendeten. Sie wurden durch einige überführte Spione aufgedeckt. In Anlehnung an Polybius-Quadrate schreibt man sie meist als Matrizen an, etwa

	0	1	2	3	4	5	6	7	8	9
	s	i	o	e	r	a	t	n		
8	c	x	u	d	j	p	z	b	k	q
9	.	w	f	l	/	g	m	y	h	v

(∗)

wobei die erste Zeile die einelementigen Chiffren enthält.

Mit $W = Z_{10}$ erhält man so 28 Chiffren, die für Z_{26} und zwei Sonderzeichen, . für 'stop' und / für Buchstaben-Ziffernwechsel[8] ausreichen.

Zur Konstruktion dieser Chiffre verwendet man ebenfalls Kennworte. *Dr. Per Meurling*, ein schwedischer *fellow traveller*, schrieb 1937 ein achtbuchstabiges Kennwort an und darunter das Restalphabet. Die Numerierung lief rückwärts. (*M. Delvayo* war ein spanischer Kommunist.)

	0	9	8	7	6	5	4	3	2	1
	m	d	e	l	v	a	y	o		
1	b	c	f	g	h	i	j	k	n	p
2	q	r	s	t	u	w	x	z	.	/

Dadurch wurden jedoch keineswegs die häufigeren Buchstaben einziffrig chiffriert. Dies war auch noch nicht so bei der Methode, die der schwedische Spion *Eriksson* 1941 verwendete: Er numerierte die Spalten nach der Alphabetordnung der im Kennwort vorkommenden Buchstaben um (vgl. 3.2.5):

	6	0	8	7	5	4	9	1	2	3
3	p	a	u	s	o	m	v	e	j	k
9	b	c	d	f	g	h	i	l	n	q
	r	t	w	x	y	z				

Das Kennwort war aus einer schwedischen Übersetzung von *Jaroslaw Hašek*'s Geschichte vom Braven Soldaten Schwejk, "Paus, som Svejk själv avbröt ..." genommen. Da aber die einziffrige Chiffrierung der häufigsten Buchstaben

[8] Weil diese Chiffrierung noch einer weiteren Chiffrierung unterworfen wird (‚Überchiffrierung', 9.2.1), wurden Ziffern durch identische Ziffernzwillinge oder gar -drillinge chiffriert — eine Sicherung gegen Übertragungsfehler.

auch die Telegraphierzeit reduziert, wurde vom NKWD ab 1940 eine dies besonders berücksichtigende Konstruktionsmethode angewandt.

Max Clausen, Funker des russischen Spions *Dr. Richard Sorge* in Tokyo, mußte den Satz *"a sin to err"* memorieren, der die acht häufigsten Buchstaben des Englischen enthält, zusammen 65.2 % (und für einen Agenten auch sonst ein guter Rat ist). Mit einem Kennwort /subway/ beginnend, wurde dann ein Rechteck ausgefüllt, sodann wurden spaltenweise von links nach rechts in der Reihenfolge ihres Auftretens durchnumeriert erst die Buchstaben der Menge {a s i n t o e r} mit 0..7 , dann der Rest mit 80..99 :

s	u	b	w	a	y
0	82	87	91	5	97
c	d	e	f	g	h
80	83	3	92	95	98
i	j	k	l	m	n
1	84	88	93	96	7
o	p	q	r	t	v
2	85	89	4	6	99
x	z	.	/		
81	86	90	94		

In diesem Beispiel ergibt sich in kompakter Schreibweise die oben unter (∗) angegebene Chiffre.

3.4.2 Für das kyrillische Alphabet eignet sich eine Einteilung in 7 einziffrige und 30 zweiziffrige, zusammen 37 Chiffren, die 5 Sonderzeichen ermöglichen. Die Methode, die der übergelaufene Agent *Hayhanen*, ein Gehilfe von *Abel*, verriet, verlangt zuerst, daß die Nachricht in der Mitte geteilt und verkehrt herum zusammengefügt wurde, damit die verwendeten Teile am Anfang und Ende (Standardfloskeln) nach innen kamen (‚russische Kopulation'). Als Kennwort diente das russische Wort SNEGOPAD („Schneefall"), dessen erste sieben Buchstaben zusammen 44,3 % Häufigkeit haben. Dann wurde das Rechteck des mit dem Kennwort SNEGOPA gebildeten Alphabets

С	Н	Е	Г	О	П	А	.	.	.
Б	В	Д	Ж	З	И	Й	К	Л	М
Р	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ы	Ь	Э	Ю	Я	.	.	.	.	.

umsortiert mit einem von Nachricht zu Nachricht wechselnden Schlüssel, der an vorbestimmter Stelle der Geheimnachricht eingefügt wird. Schließlich erfolgte noch eine Überschlüsselung (s. 9.2).

Winston Churchill nannte Rußland *"a riddle wrapped in a mystery inside an enigma"*. Dies trifft auch für die russische Kryptologie zu. Nur zögernd werden Namen und Methoden aufgedeckt.

4 Chiffrierschritte: Polygraphische Substitution und Codierung

Die einfache (monographische) Substitution erfordert eine vollständige Zerlegung des Klartextes in Einzelzeichen. Eine **polygraphische Substitution** erlaubt polygraphische Chiffrierschritte, d.h. Chiffrierschritte von der Gestalt $V^{(n)} \dashrightarrow W^{(m)}$ mit $n > 1$.

4.1 Der Fall $V^2 \dashrightarrow W^{(m)}$ von Bigramm-Substitutionen

4.1.1 Die älteste polygraphische Chiffrierung dieses Typs findet sich 1563 bei *Giovanni Battista Porta (Giambattista Della Porta)* in *De furtivis litterarum notis, vulgo de ziferis* (Abb. 30), eine $V^2 \longrightarrow W^1$. *Porta* zeigte großen Einfallsreichtum bei der Erfindung von 400 seltsamen Graphemen.

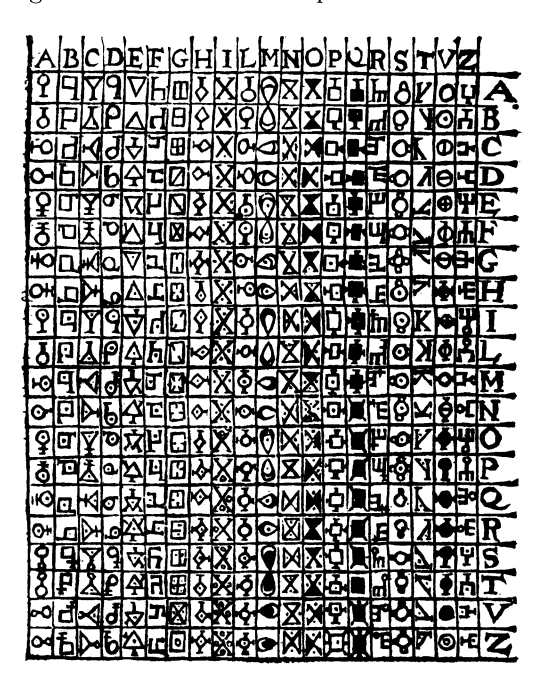


Abb. 30.
Älteste bekannte Bigramm-Substitution von *Giovanni Battista Porta*, 1563

4.1.2 Zur Darstellung der Chiffrierung $V^2 \dashrightarrow V^2$, einer bipartiten Bigramm-Substitution, wird meist eine Matrix (‚Tauschtafel') benutzt.
Für $V^2 \longleftrightarrow V^2$ handelt es sich um eine **Bigramm-Permutation**.

Nachfolgend ein Beispiel $V^2 \stackrel{2}{\longleftrightarrow} V^2$ einer *involutorischen* bipartiten Bigramm-Permutation

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o ...
a	XZ	KJ	YJ	HP	PL	EL	VB	CI	DW	XN	ZL	YP	VN	HH	CC
b	LP	QT	HE	RS	UR	CR	ZH	GV	WC	HL	YN	KT	WT	MC	KH
c	DX	MN	AO	NH	SF	GI	WL	MN	AH	GR	BZ	HS	ZU	YM	WU
d	KM	YZ	RY	FP	TR	CR	XE	JK	NY	PO	GJ	JR	PE	MO	VB
e	QU	HP	QG	JQ	YQ	OB	SA	NL	PX	OP	VS	AF	XK	XR	UQ
⋮															

Der involutorische Charakter (beispielsweise ao $\mapsto$ CC , cc $\mapsto$AO ; ah $\mapsto$ CI , ci $\mapsto$ AH ; af $\mapsto$ EL , el $\mapsto$AF) ist nicht oberflächlich erkennbar.

Involutorische bipartite Bigramm-Permutation wurde im 1940 eingeführten ‚Werftschlüssel' der Kriegsmarine benutzt, nach einem ‚Tauschtafelplan' wurden 20 Matrizen (30 ab März 1944) im täglichen Wechsel eingesetzt.

Weitere Bigramm-Permutationen $V^2 \longleftrightarrow V^2$ können wieder durch Kennwörter erhalten werden, etwa mit /amerika/ und /equality/

	a	m	e	r	i	k	b	c	d	f	g	h	j	l	n ...
e	XZ	KJ	YJ	HP	PL	EL	VB	CI	DW	XN	ZL	YP	VN	HH	CC
q	LP	QT	HE	RS	UR	CR	ZH	GV	WC	HL	YN	KT	WT	MC	KH
u	DX	MN	AO	NH	SF	GI	WL	MN	AH	GR	BZ	HS	ZU	YM	WU
a	KM	YZ	RY	FP	TR	CR	XE	JK	NY	PO	GJ	JR	PE	MO	VB
l	QU	HP	QG	JQ	YQ	OB	SA	NL	PX	OP	VS	AF	XK	XR	UQ
⋮															

(wobei natürlich der involutorische Charakter entfällt; die Dechiffrierarbeit, wenn keine inverse Tafel zur Verfügung steht, mühsamer wird).

Die Aufstellung einer Matrix erfordert die gute Arbeit eines Kryptologen, damit die Häufigkeiten der Buchstaben nivelliert (vgl. 3.1.2) werden. Auch eine Angleichung an die Häufigkeitsverteilung der Buchstaben in der betreffenden Sprache und damit die Vortäuschung einer Transposition ist möglich. Ideal ist eine Matrix, bei der in jeder Zeile und jeder Spalte jeder Buchstabe genau einmal als erster und einmal als zweiter vorkommt, etwa

AB	BC	CA		AC	BA	CB	DD		AA	BB	CC	DD	EE
CC	AA	BB	or	BD	AB	DA	CC	or	BC	CD	DE	EA	AB
BA	CB	AC		DB	CD	BC	AA		CE	DA	EB	AC	BD
				CA	DC	AD	BB		DB	EC	AD	BE	CA
									ED	AE	BA	CB	DC

Solche Matrizes heißen ‚griechisch-lateinische Quadrate'. Außer für $N = 6$ (‚Eulersches 36-Offiziere-Problem', 1779) gibt es für alle natürlichen Zahlen $N > 2$ griechisch-lateinische Quadrate, in der Regel mehrere.

Jedenfalls ist das von *Helen Fouché Gaines* angegebene Beispiel

AA BA CA DA ...
AB BB CB DB ...
AC BC CC DC ...
AD BD CD DD ...
⋮ ⋮ ⋮ ⋮

nicht geeignet: Es ergibt sich eine monographische 2-alphabetische Chiffrierung (s. polyalphabetische Chiffrierung, 8.2) mit anschließender paarweiser Buchstabenvertauschung (s. Transposition, Kapitel 6).

Nachfolgende Tabelle gibt für $N = 26$, $N = 10$ und $N = 2$ einen Überblick über die Anzahl der verfügbaren Matrizes (vgl. 3.2.6) $V^2 \leftarrow\!\!\!\rightarrow V^2$:

Anzahl der Matrizes	$Z(N)$	$Z(26)$	$Z(10)$	$Z(2)$
alle	$(N^2)!$	$1.88 \cdot 10^{1621}$	$9.33 \cdot 10^{157}$	24
echt involutorische	$\approx (N^2!)^{\frac{1}{2}}$	$7.60 \cdot 10^{809}$	$2.73 \cdot 10^{78}$	3

K 1 Norw.	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	
a	ca	fn	bl	ou	ih	oo	il	bv	bw	er	rm	qm	mn	ab	zm	ns	wl	yc	zy	tr	du	wo	oa	ho	ic	pu	a
b	sk	wm	dg	ia	cw	pf	if	vd	da	xz	fo	dh	px	rr	iv	gh	mu	ae	qr	tb	og	sr	vu	qg	zt	pm	b
c	hp	no	ij	xp	ji	yf	eo	xh	zu	pl	ft	yv	qw	am	qp	lz	bg	be	lc	nw	ap	vx	rs	yi	wy	gi	c
d	ov	gg	tk	ys	hm	tx	eq	qa	iu	zo	ud	gj	lh	bn	fm	ta	ej	hi	jc	sv	vp	rd	br	rh	kt	tw	d
e	di	wz	qo	pz	ag	wk	fl	uo	ll	oe	ph	jq	gl	vy	lf	af	vt	cj	vq	yz	rz	fc	ps	pq	ro	aq	e
f	cu	rf	nt	xr	ya	tg	xj	db	sc	hg	zr	hs	em	xv	vr	ul	wn	sh	ku	my	va	ad	fg	zp	ut	lb	f
g	sx	hd	vk	st	lk	xf	gn	lv	yr	yd	xg	kr	hc	xl	xw	pa	au	eb	gb	li	id	rj	tz	xq	wd	rn	g
h	bq	oy	sb	mw	qx	zd	ar	po	on	rx	sj	om	as	mb	vs	ke	yy	xy	uj	hb	rc	jg	co	fq	jr	pe	h
i	cb	sl	ri	cf	qt	ek	un	kl	nx	to	hk	ew	yo	wp	kj	kh	su	xi	jo	of	dt	ml	zi	bk	qq	gu	i
j	vv	tf	fi	mp	ky	hl	qc	iq	na	gd	up	tq	hq	xs	xb	wt	ez	mm	hj	vg	eh	dc	qe	ti	uk	cg	j
k	uv	bt	bf	ux	kz	zw	ex	nh	ac	av	tt	aw	ye	dw	dy	nv	wf	dn	sf	eg	lg	wc	kx	ur	pc	od	k
l	ir	ea	kn	le	jb	nu	at	hu	zl	fw	ce	ka	jv	bm	ev	ak	cp	gm	yn	cd	kd	ue	xm	ig	fy	ht	l
m	mv	el	yg	ny	bu	cq	fk	wq	pk	oo	ms	sz	rl	pr	qi	te	qn	kf	gs	uc	kv	kc	dl	kp	cl	lp	m
n	je	sq	gz	ts	dk	vo	xo	ge	mj	qv	mi	dp	vf	rb	yj	bj	mg	vl	qs	uw	rq	pb	mh	lt	oz	qk	n
o	vc	gk	al	vz	np	vm	by	cm	re	wv	uz	yt	ww	gp	js	en	tv	jn	bo	tm	sp	or	fj	ub	ck	td	o
p	hr	ah	ik	xn	mo	zk	ds	in	dz	ym	ci	qu	dv	df	nk	yk	pt	iz	ef	ws	es	ip	fz	ss	jk	ct	p
q	ec	xc	jj	vb	vh	ot	pg	ib	ty	ch	pd	qz	qf	fd	oh	sa	bc	zj	ba	fp	nq	wa	ie	vi	oq	lw	q
r	wi	uq	ln	ja	gq	lo	rp	sd	ko	iy	si	mc	uu	io	yh	ru	xx	qy	fr	hy	ob	ox	nl	uh	fh	ga	r
s	zg	nf	sy	jw	nn	kq	vn	ld	go	mt	pn	jf	he	um	ua	za	xt	bb	op	qh	gf	yl	md	os	ju	ei	s
t	yw	wg	mx	ol	sw	se	rv	yp	us	rk	dx	zs	bz	dj	cn	mf	hx	de	it	ai	ug	mk	ql	cs	ix	pi	t
u	gy	fa	ow	gr	vw	bh	ly	kw	ry	mz	pj	sg	jz	gt	dd	nd	et	az	tp	jh	cx	iw	la	zq	rw	lm	u
v	gv	bi	oi	ii	zb	lj	hz	zh	nb	ks	cy	yq	jx	dq	ma	hf	wr	lq	jp	ng	gw	jl	rg	tl	lr	wh	v
w	aj	gx	nr	qb	uf	ok	rt	xu	bp	wb	qd	jt	mr	aa	pv	yu	nj	xd	eu	mq	hw	nz	ze	km	uy	tm	w
x	kb	yx	ui	pw	we	xk	fe	vj	gc	pp	ep	hh	zn	ha	zf	ax	do	py	nm	xe	ff	so	tc	sm	fb	fx	x
y	fs	ay	ni	wj	wu	fu	ed	an	fv	xa	cv	cz	bs	ve	th	cc	bx	ra	cr	im	ne	hn	zv	oj	yb	tj	y
z	kg	bd	wx	zz	zx	lu	jy	sn	zc	tu	is	ao	dr	ki	ls	ey	qj	ee	lx	hv	nc	dm	jd	me	jm	kk	z
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	Pnr. **0033**

Abb. 31a. Bipartite Bigramm-Chiffrierung von Rufzeichen des RSHA-Funknetzes in Norwegen

Ein klassisches Beispiel zeigt Abb. 31a, eine Chiffrierung $V^2 \leftarrow\!\!\!\rightarrow V^2$ zur Verschlüsselung von Rufzeichen des Funknetzes des RSHA in Norwegen. Es ist allerdings kein griechisch-lateinisches Quadrat.

Zehn solcher Tabellen wurden im Amt VI (*Heinz Jost*, ab 1942 *Walter Schellenberg)*, der auslandsnachrichtendienstlichen Abteilung *Himmlers*, erstellt,

möglicherweise von *Andreas Figl*.[1] Dieser, ein sehr erfahrener Kryptanalyst, hatte 1911 als Hauptmann das kryptanalytische Büro der k.u.k. Armee aufgebaut, in der besten Tradition des Wiener Hofes. 1915 löste der Major *Figl* italienische Funksprüche. 1926 stand er im Rang eines Obersten, als er ein gutes Lehrbuch „Systeme des Chiffrierens“ (243 Seiten mit 45 Beilagen, Graz 1926) schrieb. Eine angekündigte Fortsetzung „Systeme des Dechiffrierens“ wurde bereits 1926 amtlich nicht zum Druck freigegeben; nur das Inhaltsverzeichnis, nicht aber das Manuskript scheint erreichbar zu sein.

Für die Überchiffrierung der den Funksprüchen vorangestellten Spruchschlüssel auf der Marine-ENIGMA wurden seit 1. Mai 1937 involutorische bipartite Bigrammsubstitutionen verwendet. Die dazu bereitgestellten zehn Tafeln, zwischen denen gewechselt wurde — sie trugen Namen wie FLUSS (Abb. 31b), BACH, STROM, TEICH, UFER) — kannten die Briten; sie hatten sie erbeutet (u.a. *Gedania*, June 1941; *VP 5904*, Januar 1942; *U-505*, Juni 1944) oder möglicherweise gestohlen, später auch rekonstruiert. Der willkürlich gewählte Spruchschlüssel, etwa /psq/, wurde verdoppelt zu /psqpsq/ und (mit einer für den Tag geltenden Grundstellung, etwa iaf) chiffriert; das Chiffrat, etwa SWQRAF, wurde in zwei Teile aufgeteilt:

$\begin{matrix} S & W & Q & * \\ * & R & A & F \end{matrix}$ und mit Blendern aufgefüllt: $\begin{matrix} S & W & Q & X \\ P & R & A & F \end{matrix}$.

Die Bigrammchiffrierung wurde vertikal vorgenommen, mit etwa

$\begin{matrix} S \\ P \end{matrix} \leftrightarrow \begin{matrix} Q \\ A \end{matrix}$, $\begin{matrix} W \\ R \end{matrix} \leftrightarrow \begin{matrix} F \\ P \end{matrix}$, $\begin{matrix} Q \\ A \end{matrix} \leftrightarrow \begin{matrix} C \\ D \end{matrix}$, $\begin{matrix} X \\ F \end{matrix} \leftrightarrow \begin{matrix} S \\ Z \end{matrix}$

ergab sich $\begin{matrix} Q & F & C & S \\ A & P & D & Z \end{matrix}$.

Gesendet wurde der **chiffrierte Spruchschlüssel** (*indicator*) QFCSAPDZ . Empfangsseitig wurde das Verfahren rückwärts angewandt: Zuerst die (involutorische) Bigrammsubstitution und das Wegbrechen der Blender, dann die involutorische ENIGMA-Chiffrierung mit der Grundstellung iaf , die ein Muster *123123* ergeben mußte, dessen erste Hälfte der einzustellende Spruchschlüssel war. Das Verfahren zur Vereinbarung eines Schlüssels zwischen den beiden Partner (engl. *key negotiation*) mutet kompliziert genug an, um den, der es sich ausgedacht hat, in Sicherheit zu wiegen. Für die Briten waren

[1] Das RSHA hatte 1938 beim Einmarsch in Österreich den österreichischen General *Andreas Figl* (1873–1967), ehemaliger Leiter des österreichischen Dechiffrierdienstes, zusammen mit Unterlagen „erbeutet“. Dies wurde „entdeckt“ von dem jungen Österreicher *Dr. Wilhelm Höttl* (∗ 1915), 1943 stv. Leiter von Amt VI E. Leiter des Amt VI E war Walter Huppenkothen, der die Untersuchungen zum 20. Juli 1944 leitete.
Figl, bis Mitte 1941 in Berlin-Wannsee im Gewahrsam der SS, konnte sich als „Berater“ von *Höttl* einigermaßen frei bewegen. *Höttl* zog ab Mitte 1944 auch Kryptologen der ungarischen Armee heran, darunter Major *Bibo*, dem es noch 1944 gelang, in den Verkehr des europäischen Spionage-Chefs *Allen W. Dulles* mit Washington einzudringen.
Höttl spielte nach Kriegsende noch eine unrühmliche politische Rolle im österreichischen „Verband der Unabhängigen“ und in der „Wahlpartei der Unabhängigen“, die 1949 18 Mandate erzielte, dann aber zerfiel. Selbstbewußt (‘I was Hitler’s Master Spy’) schrieb er später Bücher (‘The Secret Front’, 1954 und unter dem Pseudonym *Walter Hagen* ‘The Paper Weapon’, 1955).

die Hindernisse trotzdem überwindbar. Die Schlüsselvereinbarung ist bis auf den heutigen Tag ein besonderer Schwachpunkt der Kryptographie.

Geheim!

Kennwort: Fluß

Doppelbuchstabentauschtafel für Kenngruppen — Tafel B

Prüfnr. 516

AD	AE	AJ	AK	AL	AM	BC	BD	BE	CE	CF	CG	DG
AA = RN	BA = IK	CA = KJ	DA = PK	EA = TC	FA = XP	GA = NE	HA = JR	IA = NN	JA = WE	KA = EI	LA = EU	MA = RG
B = KW	B = RT	B = PO	B = EZ	B = JX	B = OI	B = JO	B = NO	B = VF	B = OY	B = GW	B = KH	B = IP
C = FM	C = EY	C = JV	C = AW	C = OM	C = IU	C = BK	C = GY	C = DN	C = NQ	C = IM	C = VO	C = WW
D = YE	D = AK	D = BM	D = JM	D = MJ	D = RB	D = FL	D = TB	D = FW	D = KK	D = SE	D = YA	D = TA
E = NR	E = OW	E = MZ	E = WB	E = NY	E = PA	E = ZT	E = ZI	E = RP	E = TN	E = AG	E = CV	E = BQ
F = UC	F = WQ	F = EK	F = XY	F = AS	F = DZ	F = SA	F = QY	F = EO	F = VS	F = JH	F = SC	F = KV
G = KE	G = QA	G = KT	G = ZA	G = PU	G = NV	G = LR	G = OA	G = WS	G = FR	G = PN	G = JU	G = NS
H = XU	H = ZZ	H = AZ	H = BS	H = WO	H = ZK	H = TP	H = CU	H = NU	H = KF	H = DT	H = ZQ	H = VK
I = PC	I = OG	I = ND	I = MT	I = KA	I = QR	I = MW	I = QS	I = TM	I = PM	I = LV	I = RX	I = XC
J = JP	J = HQ	J = TQ	J = OE	J = GZ	J = LN	J = AU	J = IS	J = XO	J = SV	J = CA	J = WZ	J = ED
K = BD	K = GC	K = GX	K = FP	K = CF	K = EL	K = QN	K = PG	K = BA	K = IT	K = JD	K = EM	K = ZF
L = QI	L = PR	L = RE	L = RI	L = FK	L = GD	L = WH	L = KR	L = MS	L = UP	L = TO	L = OK	L = DR
M = HT	M = CD	M = WA	M = VV	M = LK	M = AC	M = PB	M = SF	M = KC	M = DD	M = BW	M = TR	M = SU
N = MR	N = NL	N = OS	N = IC	N = TY	N = CP	N = OX	N = SZ	N = QZ	N = PX	N = UX	N = FJ	N = LO
O = BZ	O = US	O = DY	O = YJ	O = IF	O = VE	O = JT	O = FY	O = YV	O = GB	O = QC	O = MN	O = NX
P = XI	P = SX	P = FN	P = NF	P = NC	P = DK	P = RY	P = MX	P = MB	P = AJ	P = VJ	P = BT	P = FZ
Q = OZ	Q = ME	Q = QF	Q = GU	Q = WV	Q = PY	Q = IZ	Q = BJ	Q = OV	Q = XH	Q = RS	Q = IV	Q = OJ
R = UK	R = YN	R = XJ	R = ML	R = KS	R = JG	R = CY	R = OP	R = SH	R = HA	R = HL	R = GG	R = AN
S = EF	S = DH	S = ZB	S = QG	S = QW	S = UE	S = RF	S = RJ.	S = HJ	S = YZ	S = ER	S = NW	S = IL
T = IY	T = LP	T = SW	T = KH	T = XD	T = SR	T = XV	T = AM	T = JK	T = GO	T = CG	T = UF	T = DI
U = GJ	U = XK	U = HH	U = WN	U = LA	U = WX	U = DQ	U = UQ	U = FC	U = LG	U = XZ	U = XW	U = BY
V = QU	V = TI	V = LE	V = HW	V = RL	V = TL	V = UM	V = LZ	V = LQ	V = CC	V = MF	V = KI	V = UT
W = DC	W = KM	W = VP	W = SO	W = SK	W = ID	W = KB	W = DV	W = PH	W = QL	W = AB	W = PW	W = GI
X = UV	X = VY	X = UG	X = NT	X = UZ	X = YS	X = CK	X = WJ	X = UD	X = EB	X = ZY	X = PP	X = HP
Y = SG	Y = MU	Y = GR	Y = CO	Y = BC	Y = HO	Y = HC	Y = VN	Y = AT	Y = TU	Y = NZ	Y = QD	Y = VD
Z = CH	Z = AO	Z = YI	Z = FF	Z = DB	Z = MP	Z = EJ	Z = YD	Z = GQ	Z = UW	Z = WP	Z = HV	Z = CE

Fortsetzung s. Rückseite!

Kennwort: Fluß

Tafel B

DH	DJ	DR	DS	DT	EG	EH	EJ	EK	EO	ER	ES	ET
NA = TZ	OA = HG	PA = FE	QA = BG	RA = QH	SA = GF	TA = MD	UA = QX	VA = ON	WA = CM	XA = TX	YA = LD	ZA = DG
B = QV	B = ZX	B = GM	B = ZD	B = FD	B = OT	B = HD	B = SD	B = MY	B = DE	B = UL	B = VG	B = CS
C = EP	C = TH	C = AI	C = KO	C = PL	C = LF	C = EA	C = AF	C = ZO	C = QJ	C = MI	C = WL	C = SI
D = CI	D = XS	D = NH	D = LY	D = OQ	D = UB	D = ZN	D = IX	D = SY	D = PV	D = ET	D = HZ	D = QB
E = GA	E = DJ	E = QT	E = TJ	E = CL	E = KD	E = YX	E = FS	E = FO	E = JA	E = WM	E = AD	E = TT
F = DP	F = QM	F = XX	F = CQ	F = GS	F = HM	F = RO	F = LT	F = IB	F = VT	F = ZL	F = OR	F = MK
G = XM	G = BI	G = HK	G = DS	G = MA	G = AY	G = WK	G = CX	G = YB	G = ZM	G = SS	G = VQ	G = RM
H = PD	H = NP	H = IW	H = RA	H = LB	H = IR	H = OC	H = ZJ	H = RK	H = GL	H = JQ	H = QQ	H = VL
I = TW	I = FB	I = ZR	I = AL	I = DL	I = ZC	I = BV	I = ST	I = XR	I = YR	I = AP	I = CZ	I = HE
J = VR	J = MQ	J = TS	J = WC	J = HS	J = PQ	J = QE	J = NM	J = KP	J = HX	J = CR	J = DO	J = UH
K = YU	K = LL	K = DA	K = SN	K = VH	K = EW	K = XN	K = AR	K = MH	K = TG	K = BU	K = WR	K = FH
L = BN	L = RZ	L = RC	L = JW	L = EV	L = VX	L = FV	L = XB	L = ZH	L = YC	L = ZP	L = SQ	L = XF
M = UJ	M = EC	M = JI	M = OF	M = ZG	M = ZV	M = II	M = GV	M = ZU	M = XE	M = NG	M = VW	M = WG
N = IA	N = VA	N = KG	N = GK	N = AA	N = QK	N = JE	N = YY	N = HY	N = DU	N = TK	N = BR	N = TD
O = HB	O = UU	O = CB	O = VZ	O = TF	O = DW	O = KL	O = TV	O = LC	O = EH	O = IJ	O = PZ	O = VC
P = OH	P = HR	P = LX	P = XT	P = IE	P = RV	P = GH	P = JL	P = CW	P = KZ	P = FA	P = ZS	P = XL
Q = JC	Q = RD	Q = SJ	Q = YH	Q = UR	Q = YL	Q = CJ	Q = HU	Q = YG	Q = BF	Q = YT	Q = RW	Q = LH
R = AE	R = YF	R = BL	R = FI	R = WU	R = FT	R = LM	R = RQ	R = NJ	R = YK	R = VI	R = WI	R = PI
S = MG	S = CN	S = UY	S = HI	S = KQ	S = XG	S = PJ	S = BO	S = JF	S = IG	S = OD	S = FX	S = YP
T = DX	T = SB	T = WY	T = PE	T = BB	T = UI	T = ZE	T = MV	T = WF	T = OU	T = QP	T = XQ	T = GE
U = IH	U = WT	U = EG	U = AV	U = ZW	U = MM	U = JY	U = OO	U = YW	U = RR	U = AH	U = NK	U = VM
V = FG	V = IQ	V = WD	V = NB	V = SP	V = JJ	V = UO	V = AX	V = DM	V = EQ	V = GT	V = IO	V = SM
W = LS	W = BE	W = LW	W = ES	W = YQ	W = CT	W = NI	W = JZ	W = YM	W = MC	W = LU	W = VU	W = RU
X = MO	X = GN	X = JN	X = UA	X = LI	X = BP	X = XA	X = KN	X = SL	X = FU	X = PF	X = TE	X = OB
Y = EE	Y = JB	Y = FQ	Y = HF	Y = GP	Y = VD	Y = EN	Y = PS	Y = BX	Y = PT	Y = DF	Y = UN	Y = KX
Z = KY	Z = AQ	Z = YO	Z = IN	Z = OL	Z = HN	Z = NA	Z = EX	Z = QO	Z = LJ	Z = KU	Z = JS	Z = BH

Abb. 31b. Involutorische Bigrammsubstitution FLUSS der Kriegsmarine

Verschlüsselungstafel.

	0	1	2	3	4	5	6	7	8	9
0	23	48	60	05	78	35	58	64	29	52
1	20	77	33	59	21	70	02	40	63	08
2	11	49	01	69	47	41	79	74	22	42
3	32	76	39	18	75	30	09	51	80	65
4	61	19	43	81	06	56	73	62	10	28
5	85	50	24	88	31	84	27	90	55	57
5	03	91	96	53	68	16	44	89	15	87
7	97	25	71	04	95	34	14	37	93	38
8	26	72	54	92	13	83	45	00	66	67
9	86	12	98	36	99	46	82	17	94	07

Entschlüsselungstafel.

	0	1	2	3	4	5	6	7	8	9
0	87	22	16	60	73	03	44	99	19	36
1	48	20	91	84	76	68	65	97	33	41
2	10	14	28	00	52	71	80	56	49	08
3	35	54	30	12	75	05	93	77	79	32
4	17	25	29	42	66	86	95	24	01	21
5	51	37	09	63	82	58	45	59	06	13
6	02	40	47	18	07	39	88	89	64	23
7	15	72	81	46	27	34	31	11	04	26
8	38	43	96	85	55	50	90	69	53	67
9	57	61	83	78	98	74	62	70	92	94

Abb. 32. Bipartite Bigramm-Chiffrierung (‚Geheimklappe') zur Überchiffrierung von Ziffern-Codes

Die Briten sollten durch ihre eigenen Erfolge gewarnt sein: Auch die britische Merchant Navy benutzte Bigrammsubstitution zur Überchiffrierung ihres praktisch offenen BAMS-Code. Die Chiffrierunterlagen fielen 1940 in deutsche Hände, als der deutsche Hilfskreuzer *Atlantis* das Schiff *City of Bagdad* im Indischen Ozean aufbrachte. Dem B-Dienst der Kriegsmarine gelang es bis 1943, die Überchiffrierung der alliierten Handelsschiffs-Funksprüche abzustreifen.

Zur Überchiffrierung von Ziffern-Codes dient eine Chiffrierung $Z_{10}^2 \longleftrightarrow Z_{10}^2$, wie sie die ‚Geheimklappe' bietet, die im März 1918 von den Deutschen für taktische Nachrichten an der Westfront eingeführt wurde, mit einer Tafel zur Chiffrierung und einer zur Dechiffrierung (Abb. 32). Gegen Ende des 1. Weltkriegs wurde diese bipartite Bigrammsubstitution täglich gewechselt.

4.1.3 Auch tripartite Bigrammsubstitutionen $V^2 \longrightarrow W^3$ werden gelegentlich benützt, etwa die denäre tripartite Bigramm-Substitution ($W = Z_{10}$)

	a	b	c	d	e	...
a	148	287	089	623	094	...
b	243	127	500	321	601	...
c	044	237	174	520	441	...
d	143	537	188	257	347	...
⋮	⋮	⋮	⋮	⋮	⋮	

Kryptanalytisch fällt $V^2 \dashrightarrow W^{(n)}$ für beliebiges n in ein und die selbe Klasse und kann aufgefaßt werden als $|V|$-fach homophone einfache Substitution der gerade numerierten bzw. der ungerade numerierten Buchstaben. Entsprechend trivial ist es, die Chiffrierung zu brechen, wenn, wie im obigen Beispiel $V^2 \longleftrightarrow V^2$ von *Helen Fouché-Gaines*, ohne Verwendung eines Kennworts gearbeitet wird und ziemlich viel Material vorliegt. *Eyraud* weist darauf hin, daß insbesondere die Methode, eine Nachricht in zwei Hälften geteilt untereinanderzuschreiben und für spaltenweise Paare Bigramm-Substitution zu verwenden, eine *complication illusoire* ist.

4.2 Spezialfälle von Playfair und Delastelle: Tomographische Verfahren

4.2.1 1854 erfand *Charles Wheatstone* eine spezielle bipartite Bigramm-Substitution (Abb. 33), die sein Freund *Lyon Playfair, Baron of St. Andrews*, hohen Regierungsstellen und Militärs empfahl. Das System wurde erstmals im Krimkrieg verwendet, *Playfair*s Name blieb mit ihm verbunden. Noch im 1. Weltkrieg benutzte die britische Armee dieses System, und die Deutschen brachen es ab Mitte 1915 regelmäßig.

Der PLAYFAIR-Chiffrierschritt geht wie folgt: Ein aus einem Kennwort gewonnenes permutiertes Alphabet Z_{25} (etwa das klassische Z_{26} unter Wegfall des J) wird in ein 5×5-Quadrat (frz. *damier*) geschrieben:[2]

P	A	L	M	E		T	O	N	R	S
R	S	T	O	N		D	F	G	B	C
B	C	D	F	G	or	K	Q	U	H	I
H	I	K	Q	U		X	Y	Z	V	W
V	W	X	Y	Z		L	M	E	P	A

und dieses als Torus geschlossen gedacht. Stehen nun die beiden Buchstaben eines Bigramms in ein und der selben Zeile bzw. Spalte, so nimmt man für jeden den rechten bzw. unteren Nachbarn, im linken Beispiel

am ↦ LE bzw. tx ↦ DL

Ist das aber nicht so, so nimmt man statt des ersten Buchstabens den in der selben Zeile, aber in der Spalte des zweiten Buchstabens liegenden und statt des zweiten Buchstabens den in der selben Zeile, aber in der Spalte des ersten Buchstabens liegenden Buchstaben (‚Überkreuz-Schritt')

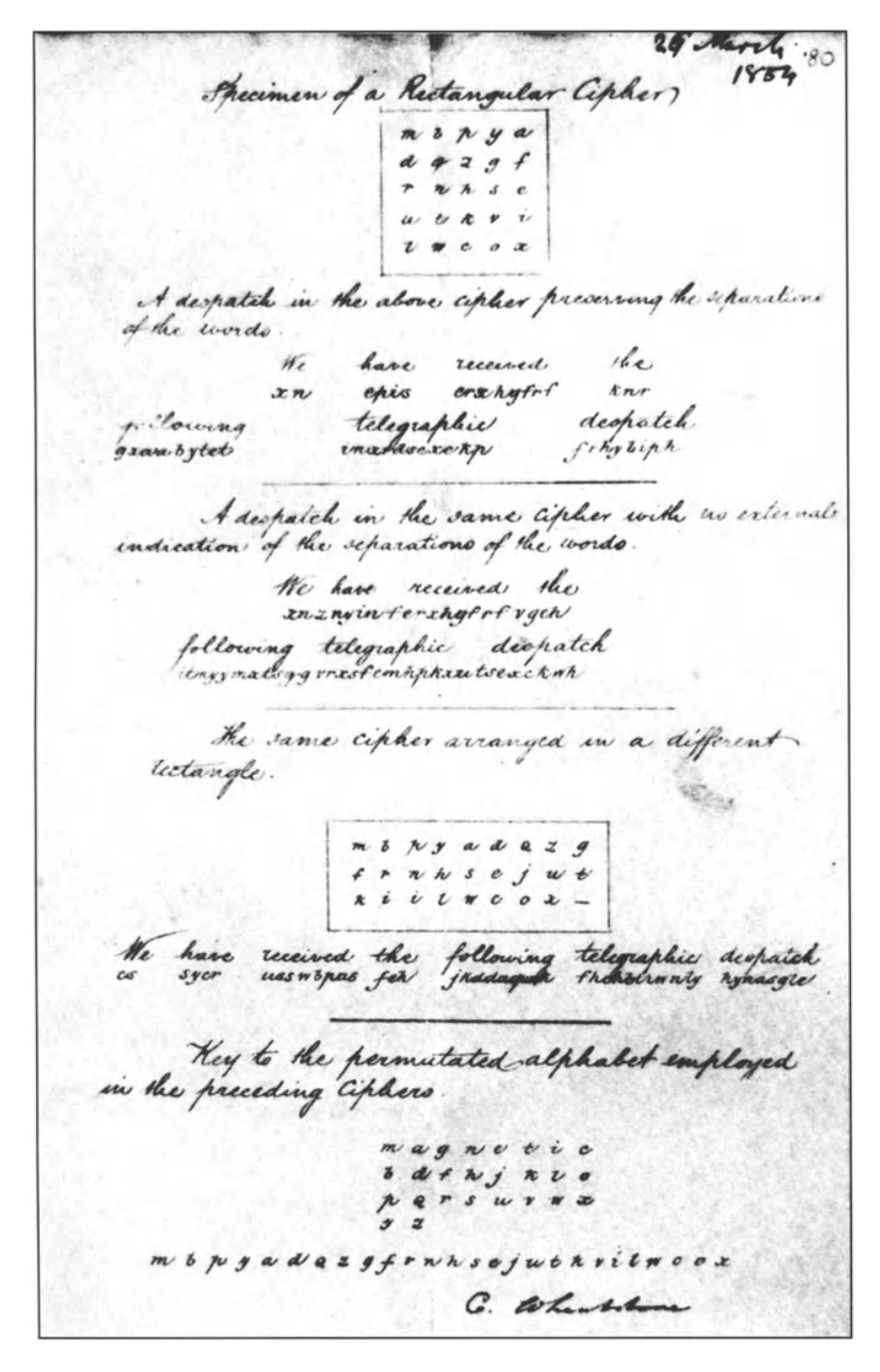
ag ↦ EC

Durch Einschub von x werden Bigramme mit Doppelzeichen vermieden, ba ll oo n wird durch ba lx lo on ; le ss se ve n wird durch le sx sx se ve n ersetzt. *Matteo Argenti*s Rat, Buchstabenverdopplungen zu unterdrücken, war vergessen. Der PLAYFAIR-Chiffrierschritt besticht jedoch ob seiner Einfachheit. Seine kombinatorische Komplexität ist allerdings wegen der Torussymmetrie sogar kleiner als die einer einfachen Substitution.

Im obigen dritten Fall kann das Playfair-Verfahren gedeutet werden als Zusammensetzung von Abbildungen: Einer Abbildung des Urtextzeichenpaars in ein Paar von Zeilen- und Spaltenkoordinaten, einer Permutation der Spalten-Koordinaten und einer Rückübersetzung in ein Urtextpaar (ähnlich einem Schüttelreim, s. 6.1.2)

a g
12 35
×
15 32
E C

[2] *Wheatstone* benutzte ursprünglich Alphabete, die nach der in 3.2.5 geschilderten Art besser durchmischt waren, und auch rechteckige Anordnungen. Diese wichtigen Sicherheitsmaßnahmen fielen jedoch bald unter den Tisch.



26 March 1854 ·80

Specimen of a Rectangular Cipher

m b p y a
d q z g f
r n h s e
u t k v i
l w c o x

A despatch in the above cipher preserving the separations of the words.

We have received the
xn epis crxhgfrf knr

following telegraphic despatch
graubytet imxrasexckp frhgbiph

A despatch in the same cipher with no external indication of the separations of the words.

We have received the
xnznyinferxhgfrfvgch

following telegraphic despatch
iengymatsygrrxsfemnpkxutsexckmh

The same cipher arranged in a different rectangle.

m b p y a d q z g
f r n h s e j u t
k i v l w c o x –

We have received the following telegraphic despatch
cs sycr uaswbpas fch jkddaquh fhcbsirnnty hynasgle

Key to the permutated alphabet employed in the preceding Ciphers.

m a g n e t i c
b d f h j k l o
p q r s u v w x
y z

m b p y a d q z g f r n h s e j u t k v i l w c o x

C. Wheatstone

Abb. 33. Beschreibung des sogenannten Playfair-Verfahrens, signiert von *Charles Wheatstone*, 26. März 1854

Solche Zusammensetzungen von Chiffrierungen, die auf eine Zerlegung und Wiederzusammensetzung hinauslaufen, heißen **tomographische Verfahren** (engl. *fractionating ciphers*, frz. *chiffres à damiers*, *Auguste L. A. Collon* 1899), wir werden auf sie in 9.4.4 zurückkommen.

4.2.2 Ein modifiziertes Playfair-Verfahren wurde im Heer und im SD ab Mitte 1941 als „Handschlüssel“ verwendet – und von den Briten unter Brigadier *John H. Tiltman* († 1984) bis Herbst 1944 regelmäßig gebrochen. Genannt ‚Doppelkas[set]tenverfahren‘ oder auch ‚2-Tafel-PLAYFAIR‘ (engl. *double casket, double* PLAYFAIR), gebrauchte es (etwa unter Wegfall des J) zwei verschiedene 5×5-Quadrate, beispielsweise

A	Y	K	I	H		Y	X	U	H	A
L	B	M	N	P		T	R	K	B	I
Q	R	C	O	G		P	M	C	G	S
Z	X	V	D	S		F	D	L	Q	V
F	W	U	T	E		E	N	O	W	Z

die nicht nach einem Kennwort, sondern „zufällig“ gebildet und dann verteilt worden waren. Chiffrierschritte wie

$$\text{ah} \mapsto \text{AY} \quad , \quad \text{nr} \mapsto \text{KP} \; , \quad \text{nb} \mapsto \text{IP}$$

treten auf, wenn Klartextzeichen in der selben Zeile stehen, sonst wird ein Überkreuz-Schritt

$$\text{xe} \mapsto \text{FW} \quad , \quad \text{or} \mapsto \text{MN} \; , \quad \text{bx} \mapsto \text{RY}$$

verwendet. Der Klartext wurde überdies in Gruppen einer vorgegebenen Länge, üblicherweise 17, zerschnitten: die Nachricht (*Noel Currer-Briggs*)

anxobergruppenfuehrerxvonxdemxbachxkiewxbittexdreixtausendxschuss
xpatronenxschickenstop

mit /x/ für den (nicht unterdrückten!) Wortzwischenraum wurde in Zeilen von 17 Zeichen zerlegt und je zwei Zeilen wie folgt in Zeichenpaaren chiffriert

a	n	x	o	b	e	r	g	r	u	p	p	e	n	f	u	e	
h	r	e	r	x	v	o	n	x	d	e	m	x	b	a	c	h	
A	K	F	M	R	Z	C	M	M	N	T	R	N	I	Z	O	W	
Y	P	W	N	Y	S	W	E	Y	V	E	G	H	P	A	C	H	usw.,

Die Prozedur wurde einmal wiederholt: ay ↦ XY , kp ↦ YC , fw ↦ ZW , . . . dies ergab, abgeteilt in Fünfergruppen, den schließlichen Geheimtext

XYYCZ WRUPY VQGUT UTKID . . . .

Das Verfahren war, wie das klassische PLAYFAIR, mühsam und fehleranfällig; von den zahlreichen Rückfragen und Kompromittierungen, die den nachlässigen Deutschen unterliefen, profitierten die Briten ebenso wie von der preußischen Vorliebe, ‘*methodical and courteous*’ zu sein und in Titeln und anderen Formalitäten zu schwelgen.

4.2.3 Ein tomographisches Verfahren in Reinkultur[3] wurde 1901 von *Félix Marie Delastelle* angegeben: Eine bipartite Chiffre, dann eine Transposition über vier Plätze, dann eine Rückübersetzung einer bipartiten Chiffre, etwa

[3] *Kahn*: “while searching for a method of digraphic encipherment that did not require cumbersome 26×26 enciphering tables”.

	1	2	3	4	5
1	B	O	R	D	E
2	A	U	X	C	F
3	G	H	I	J	K
4	L	M	N	P	Q
5	S	T	V	Y	Z

o n
12 ╳ 43
14 ╳ 23
D X

oder

o n
1 4 D
2 3 X

Der Chiffrierschritt ist involutorisch und ergibt eine bipartite Bigramm-Substitution, ähnlich der in 4.1.2. Für die Rückübersetzung kann auch ein anderer, **konjugierter** Chiffrierschritt verwendet werden.

Vor einer *complication illusoire* muß gewarnt werden: Eine bloße Verschiebung um eine Stelle, ein ‚Kulissenverfahren' (Rohrbach 1948) bringt nicht den erwarteten Effekt:

... a b s a l o m ...
3 2 1 1 1 5 1 2 1 4 1 1 2 4 2 3
H B E O D B C X

Der unbefugte Entzifferer braucht gar nicht das Quadrat zu rekonstruieren: Er betrachtet die Chiffre als $V \dashrightarrow V^2$ mit Homophonen

$$a \mapsto \left.\begin{matrix} O\\U\\H\\M\\T \end{matrix}\right\} \times \left\{\begin{matrix} B\\O\\R\\D\\E \end{matrix}\right. , \quad b \mapsto \left.\begin{matrix} B\\A\\G\\L\\S \end{matrix}\right\} \times \left\{\begin{matrix} B\\O\\R\\D\\E \end{matrix}\right. , \quad s \mapsto \left.\begin{matrix} E\\F\\K\\Q\\Z \end{matrix}\right\} \times \left\{\begin{matrix} B\\O\\R\\D\\E \end{matrix}\right. , \ldots$$

unter der Nebenbedingung des Überlappens:

a b s a l o m $\mapsto$ HB‿BE‿EO‿OD‿DB‿BC‿CX .

Dies eröffnet eine unerwartete Angriffsmöglichkeit.

Frühe Beispiele eines tomographischer Verfahrens finden sich bei *Pliny Earle Chase* (1859), s. 9.5.4 und *Alexis Koehl* (1876), s. 9.4.5 .

4.3 Der Fall $V^3 \dashrightarrow W^{(m)}$ von Trigramm-Substitutionen

4.3.1 Trigramm-Substitution in voller Allgemeinheit bereitet bereits rein technisch Schwierigkeiten: Papier ist leider nicht dreidimensional, so daß die Auflistung der Trigramme schwieriger wird, und $26^3 = 17\,576$ Trigramme sind eine beträchtliche Anzahl. Trigramm-Substitutionen sind schwerfällig zu mechanisieren. Spezielle Trigramm-Permutationen à la PLAYFAIR waren nicht sonderlich erfolgreich, ein Graf *Luigi Gioppi di Türkheim* gab 1897 ein solches System an. *Friedman* beschäftigte sich um 1920 ebenfalls mit Trigramm-Permutationen. *Jack Levine* studierte 1958 Methoden zur Trigramm-Chiffrierung, die aber nicht veröffentlicht wurden. Lineare Substitutionen (Kapitel 5) zur zur Trigramm-Chiffrierung heranzuziehen, wie es *Levine* 1963 tat, ist ein naheliegender Gedanke.

4.3.2 Eine Chiffriermaschine, die mechanisch eine quadrupartite tetragraphische Substitution durchführt, wurde 1922 für einen gewissen *Henkels* patentiert.

4.4 Der allgemeine Fall $V^{(n)} \dashrightarrow W^{(m)}$: Codes

Vorteilhafter, als bis zu 26^3=17 576 Trigramme zu chiffrieren, ist es allemal, einige Hundert, Tausend oder mehr häufig vorkommende Elemente von $V^{(n)}$ (mit ziemlich großem n) zu chiffrieren mit der Maßgabe, daß jeder Chiffrierschritt auf einer Teilmenge C von $V^{(n)}$ operiert[4]. Voraussetzung ist, daß jedes $x \in V^*$ irgendwie in Elemente aus C zerlegt werden kann:

$$x = x_1 \star x_2 \star x_3 \star \ldots \star x_k \text{ (für geeignetes } k \in \mathbb{N} \text{ und passende } x_j \in C \subseteq V^{(n)}) ,$$

und daß die ‚Einzelbuchstaben-Bedingung' $V \subseteq C$ beachtet wird, sodaß ausgefallene Wörter, einschließlich solcher aus Fachsprachen der Biologie und Chemie und Namen von Personen, Orten, Flüssen und Bergen, wenigstens buchstabenweise chiffriert werden können. Die Idee ist selbstverständlich nicht, jedes Wort in Einzelbuchstaben aufzulösen, sondern erst im Codebuch zu suchen, und auch nicht jeden Satz in Wörter aufzuspalten, sondern möglichst ganze Phrasen zu suchen – im Gegenteil, je länger der gefundene Teiltext, desto besser; umso kürzer ist dann auch die codierte Nachricht. Im übrigen kann auch eine dieser Forderung entsprechende, disziplinierte Codierung immer noch homophonisch ausfallen, aber diese freie Wahl stört nicht.

Codierdisziplin zu halten, ist jedoch schwierig. So mußte 1918 das Kommando der *American Expeditionary Force* mahnen, daß statt *boche*, mit 5 Codegruppen buchstabiert, besser *German* mit einer einzigen Codegruppe zu wählen sei und daß statt 18 Codegruppen für *almost before the crack of dawn* lediglich zwei Codegruppen für *day break* benötigt werden. Die Verwendung von Codes erfordert Intelligenz, und ihr mangelnder Gebrauch erleichtert dem unbefugten Entzifferer das Eindringen. Wenn geeignetes Personal fehlt, ist es besser, keine Codes zu gebrauchen. Im ersten Weltkrieg erwarb sich ein Leutnant *Jäger* vom Stab der 5. Armee große Verdienste um die gegnerische Seite, als er seine Anweisungen zur ‚Schlüsseldisziplin' stets mit seinem buchstabierten Namen als letztes Wort versah und sie so funken ließ. "*He was beloved by his adversaries because he kept them up with code changes,*" schreibt *Kahn*. 1918 gefährdete *Jäger* sowohl die Überchiffrierung mit der *Geheimklappe* als auch das neue Codebuch, das *Schlüsselheft*.

Der Mangel an Codierdisziplin war auf der amerikanischen Seite im 1. Weltkrieg eher noch schlimmer, nach Feststellungen von Major *Frank Moorman*, dem dafür verantwortlichen Chef von G.2 A.6. *Kahn* erklärt dies mit dem "well-known American disregard for regulations – especially ones as persnickety as these".

Im 2. Weltkrieg besserte sich die Lage geringfügig. Kryptographische Kontrolloffiziere wurden den Hauptquartieren zugeteilt. Aber da waren noch die Diplomaten. Der negative Held ist *Roosevelt*s Sonderbotschafter *Robert Murphy*, der aus Prestigegründen darauf bestand, einen diplomatischen Code

---

[4] Ein solches Chiffrierschritt-System wird nach *Kahn* Codierung genannt, wenn die Wahl von C linguistisch bestimmt ist: häufige Diphtonge, Silben, Wörter, Phrasen.

zu verwenden; durch die stereotypen Anfänge *"For Murphy"* oder *"From Murphy"* machte er es *Rohrbachs* Gruppe im Auswärtigen Amt leicht, den Code zu brechen. Fräulein *Asta Friedrichs*, die daran beteiligt war, sagte, als sie, in Marburg interniert, ihn vorbeifahren sah: „Ich wollte ihn anhalten und ihm die Hand schütteln, – so viel hatte er für uns getan".

4.4.1 Vom Abendland her gesehen, sind die ältesten Codierungen – von den Chinesen nicht als solche empfunden – die chinesischen Ideogramme. Immerhin erklärt man das Fehlen kryptologischer Errungenschaften in der alten Hochkultur Chinas damit, daß geschriebene Nachrichten ohnehin nur für wenige lesbar waren. Die Hieroglyphen jedoch bauen – 2 000 Jahre v. Chr. – auf dem Prinzip des Rebus und der Akrophonie auf: Das Bild eines "rer" (Schwein) gibt das Zeichen für den Buchstaben /r/, das Bild einer Schwalbe bedeutet sowohl "wr" (Schwalbe) wie auch "wr" (groß); eigene Zeichen (Determinative) machten, wenn nötig, den Unterschied klar. Die Hieroglyphenschrift ist in starkem Maße eine Codeschrift – wenn nötig, kann ein Wort in Einkonsonantenzeichen zerlegt werden. Lediglich der Geheimhaltungsaspekt fehlt. Aber der fehlt auch, wenn Diplomaten allmählich einen Code auswendig kennen und in der Lage sind, eine Ansprache aus dem Stegreif in diesem Code zu halten, wie der amerikanische Botschafter in Shanghai, dem dies in den zwanziger Jahren auf seinem Abschiedsdinner in GRAY (s. 4.4.7) gelang.

Wo in Ägypten Inschriften mit weniger gebräuchlichen Zeichen Seite an Seite mit Klartext zu finden sind, ist keine Geheimhaltung beabsichtigt, ganz im Gegenteil: Die pompöse Inschrift (etwa auf einem Grabdenkmal) soll beeindrucken, soll als Beschwörung geheimnisvoller magischer Kräfte wirken (Abb. 34).



Abb. 34. Hieroglypheninschriften in jeweils zwei Fassungen

Im Westen findet man um 1380 die ersten Mischungen von monographischen Substitutionen und Codierungen – zunächst nur für einige sehr häufige Wörter, darunter *et* (vgl. Abb. 26), *con, non , che* (vgl. 3.4). Als diese Zusammenstellungen etwas umfangreicher wurden, nannte man sie **Nomenklatoren**. Ein frühes Beispiel zeigt Abb. 35. Nomenklatoren behielten während der ganzen Renaissance ihre große Bedeutung. König *Charles* I. von England und Schottland benutzte einen Nomenklator mit Homophonen, den 1860 *Wheatstone* rekonstruierte: /a/ wurde durch 12 .. 17 , /b/ durch 18 .. 19 , usw., /france/ durch 9476 wiedergegeben. Um 1600 gab es Nomenklatoren mit mehreren Hundert Einträgen, numerische mit dreiziffrigen Codegruppen.

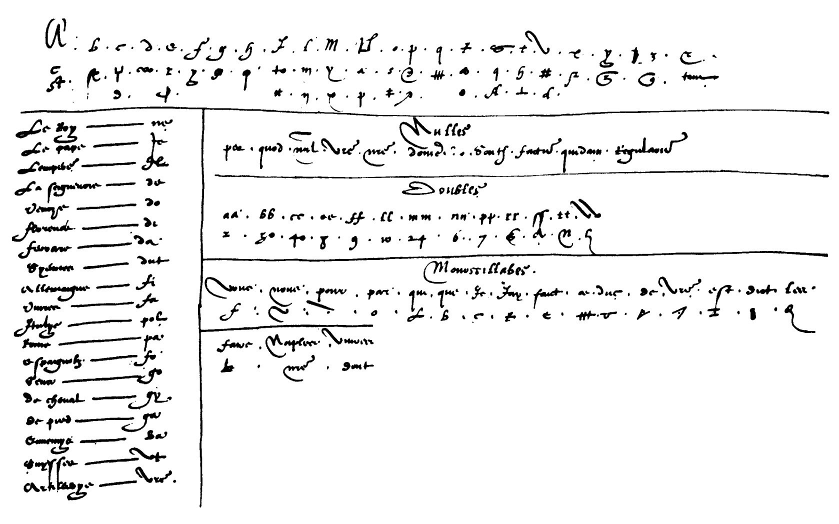


Abb. 35. Ein früher Nomenklator aus Florenz, 1554

Philipp II. *von Spanien* gab seinem Gesandten *Juan de Moreo* einen Nomenklator, der etwa 400 Codegruppen enthielt. *Viète* arbeitete vom 28. Oktober 1589 bis zum 15. März 1590 an der Entzifferung, dann konnte er seinem König *Henri* IV. die komplette Lösung geben. *Philipp*, der davon erfuhr, beschwerte sich beim Papst, daß *Henri* schwarze Magie verwandt hätte. Der Papst hingegen war besser informiert: Sein treuer Diener *G. B. Argenti* wußte Bescheid.

Im Spiel der politischen Intrigen spielten Codes fortan eine Rolle, von *Mary Stuart*'s Verurteilung 1587 bis zu den französischen Anarchisten, die im Prozeß von Saint-Etienne 1892 auf Grund von Nachrichten, die *Bazeries* entziffert hatte, überführt wurden.

Ab 1600 haben nicht nur die italienischen Staaten, sondern auch jeder der großen europäischen Höfe ihr ‚Geheimkabinett', *Cabinet Noir*, *Black Chamber*. Die Fürsten haben bedeutende Kryptologen als Helfer und Vertraute: *Louis* XIV. hatte *Antoine Rossignol*, die Zarin hatte *Christian Goldbach*, König *Charles* II. von England und Schottland hatte *John Wallis* und *Maria Theresia* einen Baron *Ignaz de Koch*. Diese Leute waren gut bezahlt und wußten um ihre Bedeutung. So schreibt *David Kahn*:

> *"Though Wallis entreated Nottingham not to publicize his solutions for fear France would again change her ciphers, as she had done nine or ten times before (probably under the expert Rossignol tutelage), word of his prowess somehow spread. The King of Prussia gave him a gold chain for solving a cryptogram, and the Elector of Brandenburg a medal for reading 200 or 300 sheets of cipher. The Elector of Hanover, not wanting to depend on a foreign cryptanalyst, got Wallis' fellow intellectual, Baron Gottfried von Leibnitz, to importune him with lucrative offers to instruct several young men in the art. When Wallis put off Leibnitz' query as to how he did these amazing things by saying that there was no fixed method, Leibnitz*

quickly acknowledged it and, hinting that Wallis and the art might die together, pressed his request that he instruct some younger people in it. Wallis finally had to say bluntly that he would be glad to serve the elector if need be, but he could not send his skill abroad without the king's leave."

Christian Goldbach (1690–1764), ab 1742 Staatsrat im russischen Außenministerium, entzifferte einen Brief des französischen Botschafters mit unerfreulichen Bemerkungen über die regierende Zarin Jelisaweta Petrowna, die Tochter Peters des Großen.

Manchmal kamen auch Mißerfolge vor, so wenn unter *de Koch* ein Brief an den Herzog von Modena irrigerweise mit dem Siegel des Herzogs von Parma wieder verschlossen wurde. Aber immerhin las die Kaiserliche Geheime Kabinetts-Kanzlei noch *Napoleon*s und *Talleyrand*s Korrespondenz.

Auch in der Neuen Welt wurde Kryptologie bedeutsam: *George Washington* hatte die Hilfe zweier Agenten, *Sam Woodhull* und *Robert Townsend*, die die Decknamen CULPER SR. und CULPER JR. führten. Sie benutzten 1779 einen Nomenklator mit ungefähr 800 Einträgen, der von Major *Benjamin Tallmadge* aufgestellt war. Auch *Thomas Jefferson* stellte 1785 als Gesandter in Paris einen Nomenklator für den späteren Präsidenten *James Madison* auf (Abb. 36).

Abb. 36. Nomenklator, 1785 von *Jefferson* für *Madison* gefertigt

4.4.2 Der oben erwähnte *Antoine Rossignol* (1600–1682) brachte um 1630 einen bedeutenden Fortschritt. Abgesehen von den frühesten Beispielen waren alle Nomenklatoren bis dahin ordnungserhaltende Abbildungen der (lexikographisch geordneten) Klartextwörter auf die (lexikographisch geordneten) Codegruppen. Damit war es möglich, im praktischen Gebrauch mit *einer* Aufstellung auszukommen — man konnte sowohl Klartextwörter wie Codegruppen in der lexikographischen Ordnung durchmustern.

Dieses System hatte jedoch einen großen Nachteil: War auch nur für *eine* Codegruppe das Klartextwort bekannt, so konnte jede Codegruppe, die dahinter lag, nur ein Klartextwort bedeuten, das ebenfalls dahinter lag. Mit mehreren erkannten Codegruppen läßt sich so eine Feineinteilung erreichen.

Erstaunlich ist nur, daß noch während des 1. Weltkriegs dieses anfällige System eines **einteiligen Codes** (engl. *one-part code*, *one-part nomenclator*, frz. *dictionaire à table unique*) Verwendung fand. So bedeutete im GREEN Code des U.S. State Department (die Codegruppen sind vom Typ $\mathcal{CVCVC}$, wo $\mathcal{C}$ ein Konsonant, $\mathcal{V}$ ein Vokal ist, mit $20^3 \cdot 6^2 = 288\,000$ Möglichkeiten)

FYTIG department MIHAk message PEDEK secured

Ein ‚Signalbuch' der deutschen Kaiserlichen Marine, das an Bord des deutschen Kreuzers *Magdeburg* im August 1914 erbeutet wurde, war einteilig und enthielt sowohl Zifferngruppen als auch Buchstabengruppen, wie nachfolgender Ausschnitt zeigt

63940	OAT	Ohnmacht, -ig
63941	OAU	Ohr, Ohren-
63942	OAÜ	Okkupation, Okkupations, -ieren
63943	OAV	Ökonomie, -isch
63944	OAW	Oktant

Rossignol führte nun gründlich durchmischte Codes ein, wobei man allerdings zur Entzifferung auch eine alphabetisch geordnete Aufstellung der Codegruppen brauchte (**zweiteiliger Code**, engl. *two-part code* , *two-part nomenclator*, frz. *dictionaire à table double*, *dictionaire à deux tables*). *Jeffersons* Nomenklator gehört dazu. Ein modernes Beispiel mit Homophonen aus dem militärischen Bereich wäre in Ausschnitten

flap	XYMAS	RATPA	ship
	TIBAL	RATPE	quite
flapjack	UPTON	RATPI	enough
flapper	UPABS	RATPO	happy
flare	OHPAP	RATPU	loxodromic

wobei für ein so häufiges Wort wie army fünf Homophone verfügbar sind:

TORMA, RAFEM, LABAR, ROMUF, IBEXO .

Ein Auszug aus einem um 1944 verwendeten deutschen ‚Satzbuch' könnte so ausgesehen haben:

a	0809	XCL	b	1479	MLA
Abend	8435	PUV	Bad	1918	TID
aber	7463	NAS	bald	1492	LGD
acht	6397	DXL	⋮	⋮	⋮
Achtung	1735	APS	z	2467	VBH
an	7958	EVG	⋮	⋮	⋮
auf	6734	UNO	zyklotron	5116	JLD
⋮	⋮	⋮			

Das ‚Kurzsignalheft' der deutschen Kriegsmarine (ab Sommer 1941) dagegen enthielt Codewörter für stereotype Befehle (engl. *caption code*) wie:

AAAA	*Beabsichtige gemeldete Feindstreitkräfte anzugreifen*
AAEE	*Beabsichtige Durchführung Unternehmung wie vorgesehen*
AAFF	*Beabsichtige Durchführung Unternehmung mit vollem Einsatz*
AAGG	*Beabsichtige Durchführung Unternehmung unter Vermeidung vollen Einsatzes*

Der ‚Wetterkurzschlüssel' der Kriegsmarine codierte u.a. Lufttemperaturen sogar *polyphon* durch einbuchstabige Codegruppen (X fehlte!):

A ≙ +28° B ≙ +27° C ≙ +26° D ≙ +25° ... W ≙ +6° Y ≙ +5° Z ≙ +4°
A ≙ +3° B ≙ +2° C ≙ +1° D ≙ 0° E ≙ −1° F ≙ −2° ... Z ≙ −21°

Auch Wassertemperatur, Luftdruck, Windrichtung, Windstärke, Sichtbarkeit, Bewölkungsgrad, geographische Breite und geographische Länge wurden in einer vorgeschriebenen Reihenfolge solcherart codiert; eine Wettermeldung bestand aus einem einzigen kurzen Wort – das war fast Klartext und führte bei Überchiffrierung zu Klartext-Geheimtext-Kompromittierungen.

4.4.3 Um 1700 hatten die Nomenklatoren 2 000 bis 3 000 Einträge, und sie wuchsen weiter an, obwohl die zweiteiligen Codebücher mehr Platz brauchten. Moderne Codes mit Homophonen und Polyphonen zeigen Abb. 37, 38 .

Shershel

– 51648 *C*...**Shershel**
– 07510 *B*...**Shetland** Islands
– 18855 *B*....Shetland Mainland
– 43026 *C*...**Shetlands**
– 53038 *A*...**Shiant** Islands
– 04216 *C*...**Shield**—*for*
– 35998 *C*...**Shielday**
– 43144 *B*...**Shielded**
– 35732 *B*....Shielded by
– 10726 *B*....Shielded from
– 53124 *C*...**Shielding**
– 06656 *B*...**Shields**—*for*—*of*
– 17848 *B*....Shields, North
– 41802 *A*....Shields, South
– 28814 *C*...**Shift**-s

268

A 10569 *B*, *B* 53472 *C*, *C* 03917 *A* } Ship is
– 35613 *A*....Ship is **not**
– 50968 *C*....Ship is **not** to
– 06679 *A*....Ship is **not** to be
– 18641 *C*....Ship is now—*at*
– 42583 *C*....Ship is to
– 10247 *A*....Ship is to be
– 53180 *C*....Ship must
– 07006 *A*....Ship must be
A 51738 *B*, *B* 41759 *C*, *C* 10994 *C* } Ship of

77

– **07700** *B*...Spontaneous-ly
– 07701 *B*...Sow-s-ing
– 07703 *B*...Rodd
– 07704 *C*...Vacate-s
– 07705 *B*...To what
– 07707 *A*...What time—*is*—*are*
A 07708 *C*...Hornet, H.M.S.
B 07708 *A*...Referring
C 07708 *B*...Wednesday
– 07709 *A*...Send-s mails for
– **07710** *C*...Worth
– 07712 *B*...Riddled by (with)
A 07713 *A*...Smoke-s—*from*—*of*
B 07713 *B*...Will be
C 07713 *C*...13th April
– 07714 *A*...Tsu Sima

– **07750** *A*...Dummy group
– 07751 *A*...Recurrences—*of*
– 07752 *B*...Report when she
– 07754 *A*...Rush-es-ing
– 07755 *C*...Purpose of
– 07756 *C*...Withdrawn from
– 07758 *B*...Sheep
A 07759 *C*...12th April
B 07759 *A*...Was no-t
C 07759 *B*...In convoy
– **07760** *C*...She could
– 07761 *A*...That every
– 07763 *A*...Sulen Isles
A 07764 *C*...Begins
B 07764 *B*...Spell word of **13 letters**
C 07764 *A*...Acknowledge

Abb. 37. Je eine Seite des homophonen Ver- und des polyphonen Entzifferungsteils des 'SA Cipher'der britischen Admiralität (1918)

Die Geheimkabinette wurden in Europa erst in der Mitte des 19. Jahrhunderts aufgelöst und damit auch das verstohlene Mitlesen diplomatischer Post beendet: 1844 in England, 1848 in Wien und Paris. Die Aufklärung hatte gesiegt. Die industrielle Revolution brachte aber den Telegraphen und damit

	総隊		海上部隊			
切	20463	各艦隊	14806		39948	
	40811	各F、各戦、各警	71731		34113	
	86660	各F、各艦、各警、長官	17487	2F 各P、▷	51395	
	04069	各F、各艦、各警、参謀長	91631	2F 附属部隊	33232	
	12951		13885		09044	
	44135	GF	84141		12682	
取	58361	GF P	57452		94906	6F
	06217	〃	41618		26430	6F
	41269	〃	14710		90258	〃
海上部隊	23623	GF 参謀長	94807	3F	16240	6F
	07384	GF 参謀	31614	3F P	08351	6F
	84098		42007	〃	94770	
	95220	GF 各P	55380	3F 参謀長	63935	
	06539	GF 各参謀長	05271	3F 参謀	44182	6F
	97614	GF 各P、▷	18519		77036	6F
	73085	GF 附属部隊	33492		00544	6F
	81754	GF 所属総潜水艦	19023	3F 各航空母艦	93973	
	99515	GF (潜水部隊欠)	20908	3F 各P、▷	03782	
	55433	GF (潜水艦欠)	63006	3F 附属部隊	20700	
	71675	GF (GKF 欠)	31558		54698	
	59249	GF 各P (GKF 欠)	60465		29424	7F
	47520	GF 各P、▷ (GKF欠)	97599		70670	7F
	95332		34511		63755	〃
	54463		27057	4F	97829	7F
	45532	1S、1F	15229	4F P	67050	7F

Abb. 38 Ausschnitt aus dem Dechiffrierungsteil eines japanischen Marine-Codes (1943)

kommerzielle Codebücher, deren Hauptaufgabe es war, die Telegramme zu komprimieren und damit den Zeitaufwand und die Kosten zu senken.

Francis O. J. Smith veröffentlichte 1845 einen Code *"The Secret Corresponding Vocabulary. Adapted for Use to Morse's Electro-Mechanic Telegraph"* — noch bevor das Morse-Alphabet eingeführt wurde. *Smith* hatte 50 000 Gruppen, und nur 67 Sätze. Seine Codegruppen waren aus Ziffern aufgebaut und sollten (s. 9.2) Überchiffrierung erlauben. Später ging man zu Codegruppen aus Buchstaben, hauptsächlich Fünfergruppen, über; die Zahl der Sätze stieg in die Hunderte, die Zahl der Gruppen bis zu 100 000. Wegen des großen Umfangs benutzte man jedoch wieder einteilige Codes, und zwar nun auch im diplomatischen Dienst, wo es auf Geheimhaltung ankam, und in militärischen Stäben. Dadurch gewannen jedoch die echten Chiffrierungen als Überchiffrierungen mehr und mehr an Bedeutung.

Hunderte kommerzieller Codes entstanden nach und nach, einer von *Henry Rogers* 1847, von *John Wills* ebenfalls 1847, dann 1874, acht Jahre nach der Fertigstellung des transatlantischen Kabels, der ABC-Code von *William Clausen-Thue*, ein Fünf-Buchstaben-Code. Andere Fünf-Buchstaben-Codes wurden von *Bolton* (*Dictionnaire pour la Correspondance Anglais*), von *Krohn* in Berlin (1873) und von *Walter* in Winterthur (1877) verbreitet.

Ein Vier-Buchstaben-Code wurde 1889 von *Katscher* in Leipzig publiziert, ein Drei-Buchstaben-Code 1874 von *Mamert-Gallian* in Paris. Andere berühmte Namen von Codeerstellern sind *John Charles Hartfield* (1877) und sein Sohn *John William Hartfield* (1890), *Henry Harvey* (1878), *Benjamin Franklin Lieber* in U.S.A.; letzterer verfaßte ein Codebuch mit 75 800 Codegruppen, das auch ins Französische und ins Deutsche übersetzt wurde. Sogar ein Sieben-Buchstaben-Code wurde publiziert, der *Ingenieur-Code* von *Galland*.

Das Bestreben war hauptsächlich, die Telegraphierkosten zu senken (*Mercantile Cypher for Condensing Telegrams*, *Buell* 1860). Dies betraf insbesondere den transatlantischen Verkehr.

Innerhalb Europa bevorzugte man, wenn eine kryptographische Absicht vorlag, die Ziffern-Codes, die einfache Überschlüsselung erlaubten. Weit verbreitetes Vorbild eines Vier-Ziffern-Codes war das *Dictionnaire abréviatif chiffré* von *F. J. Sittler* in Paris (1868) Frankreich, daneben das *Dictionnaire pour la Correspondance télégraphique secrète* von *Brunswick* in Paris (1868) und der *Dictionnaire chiffré* von *Nilac*. *Bazeries* (1893) wie auch *de Viaris* produzierten Codes; andere Vier-Ziffern-Codes waren das *Dizionario per corrispondenze in cifra* von *Baravelli* in Torino (1896), das *Chiffrier-Wörterbuch* von *Friedmann* in Berlin, und das *Chiffrierbuch* von *Steiner & Stern* in Wien (1892).

4.4.4 Die Tarifpolitik der Internationalen Telegraphen-Union (vgl. 2.5.4) führte ab 1890 zum Aufkommen von Fünf-Ziffern-Codes. Schon 1850 hatte *Brachet* in Paris ein *Dictionnaire chiffré* herausgebracht, andere waren *Diccionario para la correspondencia secreta* von *Vaz Subtil* in Lisbon (1871), *Wörterbuch* von *Niethe* in Berlin (1877) und *Dictionnaire pour la Correspondance secrète* von *N. C. Louis* in Paris (1881). Unter den späteren Codebüchern sind zu nennen das *Dictionnaire chiffré Diplomatique et Commercial* von *Airenti* und der *Telescand Code* in Frankreich, das *Diccionario Cryptographico* in Lissabon (1892), das *Nuovo Cifrario* von *Mengarini* in Rom (1898), das *Cifrario per la corrispendenza segreta* von *Cicero* in Rom (1899), *Slater's Code* von *Slater* in London (1906) und das *Clave telegrafica* von *Darhan* in Madrid (1912).

4.4.5 Im 20. Jahrhundert boten viele Codebücher sowohl Zifferngruppen wie Buchstabengruppen. Bis vor kurzem noch vielbenutzte Codes sind Bentley's (seit 1922), Rudolf Mosse Code (seit 1922), ABC 6th edition (seit 1925) sowie Peterson's Code 3rd edition von *Ernest F. Peterson*, Acme Code von *William J. Mitchel*, Lombard Code und AZ Code. Das umfangreichste Codebuch, das je in allgemeinen Gebrauch kam, wurde von *Cyrus Tibbals* für den Western Union Code zusammengestellt; es enthielt 379 300 Einträge, während der ABC Code nur 103 000 hatte.

Im Zweiten Weltkrieg benutzten die Allierten den BAMS Code ('Broadcasting for Allied Merchant Ships'), dessen Geheimhaltung weithin durchlöchert war, als Basis einer Überchiffrierung. Klartext wäre nicht schlimmer gewesen.

Der B-Dienst der deutschen Kriegsmarine hatte bis 1943 leichtes Spiel, die Bigramm-Überchiffrierung (4.1.2) der alliierten Funksprüche zu brechen.

Lange Jahre wurde in Notizbüchern ein „Internationaler Hotel-Telegraphenschlüssel für Zimmerbestellung“ abgedruckt, mit Codegruppen wie

ALBA	für ‚1 Zimmer mit 1 Bett‘,	ARAB	für ‚1 Zimmer mit 2 Betten‘,
ABEC	für ‚1 Zimmer mit 3 Betten‘,	BELAB	für ‚2 Zimmer mit je 1 Bett‘,
BIRAC	für ‚2 Zimmer mit 3 Betten‘,	BANAD	für ‚2 Zimmer mit 4 Betten‘,
CIROC	für ‚3 Zimmer mit 3 Betten‘,	CARID	für ‚3 Zimmer mit 4 Betten‘,
CALDE	für ‚3 Zimmer mit 5 Betten‘	usw.	

Der Marconi-Code von *James C. H. Macbeth* ist mehrsprachig (9 Sprachen in 4 Bänden), einen Traum von *Athanasius Kircher* verwirklichend (Abb. 39).

4.4.6 1880 führte *J. C. Hartfield* für Prüfzwecke die Zwei-Zeichen-Differenz der Codegruppen ('two-character differential') ein. Für ein 27-Zeichen-Alphabet (unter Einschluß des Zwischenraums) verbleiben bei Fünf-Buchstaben-Codes von $27^5 = 14\,348\,907$ Möglichkeiten noch $27^4 = 531\,441$, immer noch eine beträchtliche Anzahl. 1925 führt *Mitchel* auch die Sicherung gegen Zwei-Zeichen-Transposition durch ‚Dreher‘ (lieber — leiber) ein, was im vorliegenden Beispiel die Möglichkeiten nach *Rudolf Schauffler* lediglich auf 440 051 reduziert. Mitchel's Idee der 'adjacent-letter restriction' verbreitete sich dementsprechend rasch.

Die japanischen Marinecodes mit den amerikanischen Bezeichnungen JN-25A (ab 1.6.1939), JN-25B (ab 1.12.1940) benutzten fünfstellige Zahlen, die durch 3 teilbar waren. Diese Codes waren Vorläufer der fehlererkennenden und fehlerkorrigierenden Codes, die *Richard W. Hamming* 1950 einführte und die heute in den Strichcodes der Europäischen Artikel-Nummer (Gewichte abwechselnd 1 und 3, teilbar durch 10) oder in der ISBN-Numerierung (Gewichte der Reihe nach 10, 9, 8, ..., 2, 1; teilbar durch 11) allgegenwärtig sind.

4.4.7 Im Gegensatz zu kommerziellen Codebüchern, die (gegen Bezahlung) allgemein zugänglich waren und damit eine möglichst lange Lebensdauer hatten, sollten diplomatische und militärische Codes auf geplante Veralterung (2.1.1) angelegt sein und wechselten dementsprechend häufig. Sie aufzulisten ist jedenfalls unmöglich, obschon Sparsamkeit und Faulheit dem genügend raschen Wechsel oft entgegenstanden. U.S.-amerikanische diplomatische Codes, die allzulange in Gebrauch waren, sind RED und BLUE (vor 1914), beide Fünf-Ziffern-Codes, und GREEN (ab etwa 1914 bis etwa 1919), ebenfalls fünfziffrig. Um 1920 kam dann der schon in 4.4.1 erwähnte GRAY Code, von dem noch unter *Roosevelt* 1941 Gebrauch gemacht wurde. *Franklin Delano Roosevelt* sandte am 6. Dezember 1941 eine Notiz an *Cordell Hull*, den Außenminister *"Dear Cordell Shoot this to Grew* [der amerikanische Botschafter in Tokio] – *I think can go in gray code – saves time – I don't mind if it gets picked up FDR"*. Unter dem sicherheitsbewußten *Roosevelt* war schon Mitte der dreißiger Jahre der zweiteilige BROWN Code eingeführt worden; der mißtrauische Staatsmann benützte trotzdem ab 1939 Kryptosysteme des

M. N. O. P. R. S. T. U. Y. Z.
0 1 2 3 4 5 6 7 8 9

19140	UVVIM	slackness.	relâchement.	flojedad, descuido.
19141	UVVON	Slag(s).	Scorie(s).	Escoria(s).
19142	UVWEO	Slander(s).	Diffame(r), diffamation.	Calumnia(r), calumnia(s).
19143	UVWUP	slandered.	diffamé.	calumniado.
19144	UVWYR	slandering.	diffamant.	calumniando.
19145	UVYBS	slanderous.	diffamatoire.	calumnioso.
19146	UVYCT	Slate(s).	Ardoise(s).	Pizarra(s).
19147	UVYDU	Sleeper(s).	Traverse(s) (chemins de fer).	Traviesa(s), durmiente(s) (f.c.).
19148	UVYFY	Sleeve-valve.	Soupape à manchon.	Válvula de manguito.
19149	UVYMZ	Slide(s).	Glisse(r), glissière(s). tiroir de distribution.	Resbala(r), corredera(s). válvula de distribución, de corredera.
19150	UVYUM	slide-valve.	glissant, à coulisse.	resbalando, resbalamiento, deslizamiento.
19151	UVYYN	sliding.		
19152	UVYWO	sliding scale.	échelle mobile.	escala móvil.
19153	UVYZP	Slight.	Léger, peu important.	Ligero, leve.
19154	UVZUR	slightest.	le (la) moindre.	lo más ligero, leve.
19155	UVZYS	not the slightest.	pas le (la) moindre.	ni lo más ligero, mínimo.

M. N. O. P. R. S. T. U. Y. Z.
0 1 2 3 4 5 6 7 8 9

19140	UVVIM	slackness.	Schlaffheit, Geschäftsstille.	slapheid, stilte.
19141	UVVON	Slag(s).	Schlacke(n).	Schuim, slak(ken), metaalschuim(-slakken).
19142	UVWEO	Slander(s).	Verleumden(-e,-t), Verleumdung(en).	Belasteren, belaster(t), laster.
19143	UVWUP	slandered.	verleumdet.	belasterd.
19144	UVWYR	slandering.	verleumdend.	belasterend.
19145	UVYBS	slanderous.	verleumderisch.	lasterlijk.
19146	UVYCT	Slate(s).	Schiefer, Schiefertafel(n).	Lei(en).
19147	UVYDU	Sleeper(s).	(Bahn-)Schwelle(n).	Dwarsligger(s).
19148	UVYFY	Sleeve-valve.	Muffenventil.	Mofklep.
19149	UVYMZ	Slide(s).	Gleiten(-e, -et), Gleitbahn(en), Gleitführung(en).	Glijden(-t); schuif (schuiven), leibaan (leibanen), windklep(pen).
19150	UVYUM	slide-valve.	Schieberventil, Ventilschieber.	schuif, stoomschuif, schuifklep.
19151	UVYYN	sliding.	gleitend.	verschuifbaar, glijdend.
19152	UVYWO	sliding scale.	Gleitskala.	kalibermaat, proportioneele schaal.
19153	UVYZP	Slight.	Gering, von geringer Wichtigkeit.	Gering, onbeduidend.
19154	UVZUR	slightest.	geringst.	geringste.
19155	UVZYS	not the slightest.	nicht das (der, die) geringste.	niet de (het) geringste.

Abb. 39. Der Marconi-Code: Korrespondierende Buchseiten aus der Englisch-Französisch-Spanischen und der Englisch-Deutsch-Niederländischen Ausgabe

Navy Departments "*for matters of utmost secrecy*", wie er es ausdrückte. Weitere Codes: A-1, B-1, C-1, D-1 hatten *Roosevelts* Meinung von der Unsicherheit der diplomatischen Codes nicht ändern können. Der BLACK Code erschien um 1940.

Manchmal erleben die Hersteller von Codes Überraschungen: Als die *American Expeditionary Force* (A.E.F.) 1917 in Frankreich in den 1. Weltkrieg eingriff, stellte sich der 1915 herausgegebene *War Department Telegraph Code* ebenso als unsicher wie als unzureichend für taktischen Gebrauch heraus. Eiligst wurde von der *Code Compilation Subsection* des MI-8 im Juli 1917 mit der Arbeit an einem passenden Code begonnen; nach einem Jahr war er am 1. Juli 1918 fertig. Der *Military Intelligence Code No. 5* war nur ein einteiliger Code, mit Zwei-Zeichen-Differenz der Codegruppen vom Typ $\mathcal{VCVCV}$, $\mathcal{VCCVC}$ oder $\mathcal{CVCCV}$. Obwohl bald darauf ein besserer, zweiteiliger Code (*Military Intelligence Code No. 9*) verfügbar war, blieb *No. 5* bis 1. September 1934 mit der Klassifikation 'SECRET' in Gebrauch, dann wurde er mit der Kurzbezeichnung SIGCOT zu 'CONFIDENTIAL' abgestuft. Gleichermaßen wurde *No. 9*, der um 1923 eingezogen worden war, am 1. April 1933 (zu 'CONFIDENTIAL' abgestuft) neu ausgegeben; mit der Kurzbezeichnung SIGSYG für den Chiffrier-, SIGPIK für den Dechiffrier-Teil. Geldmangel war dafür verantwortlich; aber nicht einmal eine Überchiffrierung, die nur Arbeit gekostet hätte, wurde vorgeschrieben.

4.4.8 Im Bereich der unteren militärischen Gefechtsebene waren Codes mal mehr, mal weniger gut angeschrieben. Das kaiserliche Heer ging 1917 von den dafür benutzten Drehrastern (s. 6.1.4) zu Codes über. Für den Verkehr in der 3-km-Frontzone wurde im März 1917 ein einfacher Bigramm-Code 00 („Befehlstafel") eingeführt. Die Franzosen hatten schon 1916 ein *carnet de chiffre* herausgebracht, mit einem Zwei-Ziffern-Code, und bald zu einem Drei-Buchstaben-Code *carnet réduit*, mit Namen wie *olive* und *urbain*, ausgeweitet. Die Codegruppen waren nach Rubriken, wie Infanterie, Artillerie, Zahlen, Uhrzeiten, gebräuchliche Wörter, Ortsnamen, Decknamen usw. eingeteilt (engl. *caption codes*).

Im März 1918 machte das kaiserliche Heer dann den von den Alliierten vorausgesehenen Schritt zu einem überchiffrierten, aber immer noch einteiligen Code, einem Drei-Ziffern-Code. Die Überchiffrierung erstreckte sich nur auf die ersten beiden Ziffern und geschah mit der „Geheimklappe" (4.1.2), die häufig gewechselt wurde. Die feststehende dritte Ziffer gab der unbefugten Entzifferung durch das Auftreten von Mustern eine Einbruchsmöglichkeit.

Für höhere Ansprüche an Chiffriersicherheit, außerhalb der 3-km-Zone, wurde im Juni 1917 ein zweiteiliger Drei-Buchstaben-Code eingeführt („Satzbuch"). Er wurde nicht überchiffriert; seine kryptanalytische Sicherheit war von Anfang an ganz auf geplante Veralterung (etwa 14 Tage) ausgerichtet. Er enthielt zahlreiche Homophone (KXL, ROQ, UDZ für „Anschluß fehlt") und Nullen. Er wurde von den Alliierten KRU Code genannt, weil alle Codegruppen mit einem der drei Buchstaben K, R, U begannen, oder auch *Fritz* Code. Später wurden Codegruppen hinzugefügt, die mit S begannen (KRUS Code) und weiterhin solche, die mit A begannen (KRUSA Code); schließlich wurden die 26 Alphabetzeichen noch durch die Umlaute Ä, Ö, Ü ergänzt (dieser Code wurde dummerweise KRUSÄ Code genannt). Der Waffenstillstand in November 1918 beendete diese unfriedliche Epoche der *trench codes*. Aber sie waren noch nicht vergessen. In einem Manual des United States War Department von 1944 steht:

> "*Cipher machines cannot, as a rule, be carried forward of the larger headquarters, such as Division. Hence, code methods may predominate in the lower echelons and troop formations.*"

Man kann das auch so lesen, daß im militärischen Verkehr Codes ohne Überchiffrierung nur auf der untersten Stufe der Sicherheit Verwendung finden dürfen. In der U.S.Army war deshalb von *Friedman* als *'field cipher'* polyalphabetische Chiffrierung mit einem handlichen Gerät, mit der M-94 (s. 7.4.3), eingeführt worden.

Während des Zweiten Weltkriegs genügte auch das in den U.S.A. nicht mehr. Boris Hagelin, der im Mai 1940 buchstäblich in letzter Minute von Schweden über Deutschland nach Genua gereist und an Bord der *Conte di Savoia* gegangen war, erreichte die U.S.A. mit zwei seiner Maschinen C-36 (s. 8.5.1) im Gepäck und mit Plänen für die Verbesserung C-38. Dort beeindruckte er den einflußreichen *Friedman* so sehr, daß sich das *Signal Corps* nach einem

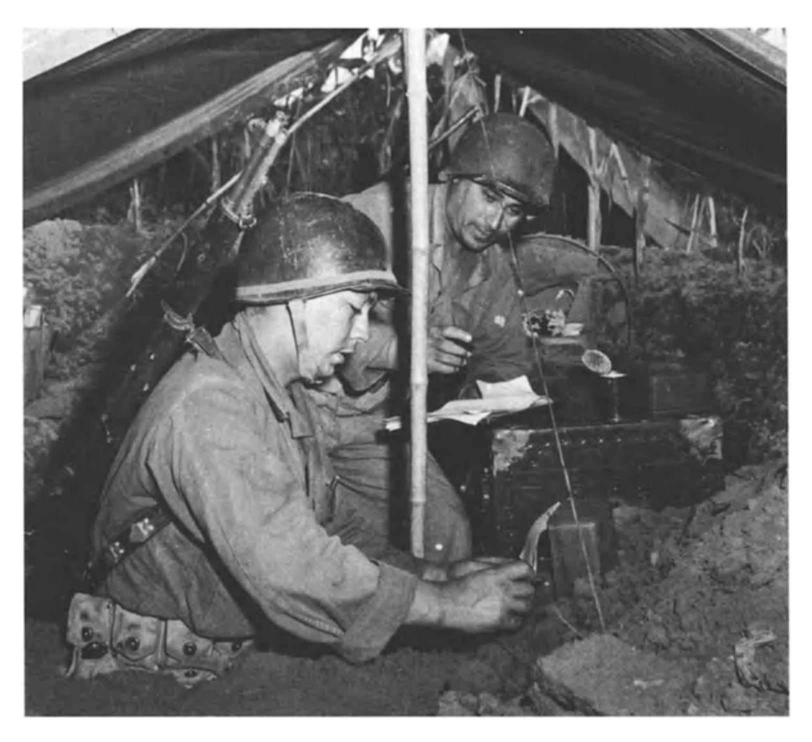


Abb. 40. C-38 von *Hagelin* (M-209) im Fronteinsatz

Test, der sich über ein volles Jahr hinzog, im Juni 1941 für einen Nachbau auf Lizenz-Basis entschied, der die Bezeichnung M-209 bekam. Die U.S. Streitkräfte gingen damit auf taktischem Niveau zu einer mechanischen Chiffriermaschine über, die auch noch nach dem Krieg verwendet wurde. Abb. 40 zeigt auf einem Gefechtsstand der 3. U.S. Infanterie-Division in Hyopchong, Korea, am 1. Oktober 1951 einen Nachrichtensoldaten mit umgehängtem Gewehr beim Gebrauch einer *Hagelin*schen M-209.



Spruchtarngerät STG-61

Dabei hatte *Hagelin* schon früh den Gebrauch von mechanischen Chiffriermaschinen in der vordersten Linie ins Auge gefaßt. Für seine C-35 wurde die Bodenplatte „so geformt, daß sie beim Gebrauch im Felde auf das Knie des Operateurs geschnallt werden konnte. Der Operateur konnte sogar, falls notwendig, mit der angeschnallten Maschine marschieren" (*Boris Hagelin*, 1979). Für die französische Gendarmerie konstruierte *Hagelin* in den fünfziger Jahren sogar eine Taschen-Chiffriermaschine etwa gleicher Leistungsfähigkeit (CD-55, CD-57), die in Verbindung mit Schlüsselstreifen als ‚Spruchtarngerät STG-61' in der Bundeswehr Verwendung fand.

Auf die Arbeitsweise der Chiffriermaschinen werden wir im 7. und 8. Kapitel zurückkommen.

5 Chiffrierschritte: Lineare Substitution

"Although Hill's cipher system itself saw almost no practical use, it had a great impact upon cryptology."
David Kahn, 1967

Eine **lineare** (‚affine') **Substitution** ist eine spezielle polygraphische Substitution. Der injektive Chiffrierschritt einer polygraphischen Blockchiffrierung

$$\chi \; : \; V^n \dashrightarrow W^m$$

mit vergleichsweise großem n und m wird auf besondere Weise eingeengt: Die endlichen Zeichenvorräte V und W werden nunmehr *wesentlich* als linear geordnete Alphabete aufgefaßt. In dieser jeweiligen Ordnung kann dann zu jedem Zeichen x das ‚nächste' Zeichen **succ** x angegeben werden, wobei zu einem **letzten Element** ω ein **erstes Element** α ‚nächstes' sein soll: $\mathbf{succ}\,\omega(V) = \alpha(V)$. Damit ist auch die Umkehrung **pred** von **succ** definiert, mit **pred** $\alpha(V) = \omega(V)$. Man sagt dann, man habe ein **Standardalphabet** ausgezeichnet. Es handelt sich dabei um eine endliche zyklische lineare Quasiordnung des Alphabets.

Es wird nun in $V = Z_{|V|}$ bzw. $W = Z_{|W|}$ eine **Addition** eingeführt. Sie kann rekursiv definiert werden: Für $a,\ b \in V$ bzw. $\in W$ gilt

$$\begin{aligned} a + b &= \mathbf{succ}\ a + \ \mathbf{pred}\ b \ , \\ a + \alpha &= a \ . \end{aligned}$$

Dies bedeutet, daß $Z_{|V|}$ bzw. $Z_{|W|}$ eindeutig und ordnungserhaltend auf $\mathbb{Z}_{|V|}$ bzw. $\mathbb{Z}_{|W|}$ abgebildet worden sind, wo $\mathbb{Z}_N$ die Gruppe der Restklassen von $\mathbb{Z}$ *modulo* der natürlichen Zahl N ist, geordnet durch Repräsentanten in der Reihenfolge 0 , 1 , $\ldots$ $N-1$; der Addition in V bzw. W entspricht dann die Addition der Restklassen. Weithin ist es üblich, das Alphabet $\{\alpha\ , \ldots\ \omega\}$ geradezu mit den **Zykelzahlen** (‚zyklotomische Zahlen') $\{0\ , \ \ldots\ , \ N-1\}$, wo $N = |V|$ bzw. $N = |W|$ ist, zu identifizieren[1]. Die Addition in V bzw. W wird nun auf V^n bzw. W^m komponentenweise übertragen.

[1] Für $Z_{26} \leftrightarrow \mathbb{Z}_{26}$ somit die Identifizierung (*'algebraic alphabet'*)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Von einer Abbildung Φ kann verlangt werden, daß sie injektiv und **additiv** ist: $\forall\, x,\ y \in \mathbb{Z}_N^n :\ \Phi(x+y) \;=\; \Phi(x)+\Phi(y)$,

in Worten: „Das Bild der Summe ist Summe der Bilder“. Es gilt dann auch

$$\forall\, x \in \mathbb{Z}_N^n \ :\ \Phi(x+x+\ldots+x) \;=\; \Phi(x)+\Phi(x)+\ldots+\Phi(x)\ ,$$

in Worten: „Das Bild eines Vielfachen ist Vielfaches des Bildes“.

In der Tat ist $\mathbb{Z}_N$ ein Ring, $\mathbb{Z}_N^n$ ein Vektorraum mit dem Nullvektor 0; die Forderung der Additivität zusammen mit der Injektivität bewirkt, daß Φ eine *reguläre* lineare Abbildung des Vektorraums $\mathbb{Z}_{|V|}^n$ in den Vektorraum $\mathbb{Z}_{|W|}^m$ ist, die auf ihrem Bild eine eindeutige Umkehrung Φ^{-1} besitzt.

Falls $N = p$ Primzahl ist, und nur dann, ist $\mathbb{Z}_N$ sogar ein Körper, das Galoisfeld $\mathbb{F}(p)$. Wir werden jedoch im folgenden zunächst die Primalität von N nicht benötigen.

Wir setzen im weiteren $W = V = \mathbb{Z}_N$ voraus und nehmen als Breite $m = n$. Dann ist eine reguläre lineare Abbildung Φ sogar bijektiv.

Wir benützen ferner eine quadratische Matrix T über $\mathbb{Z}_N$ zur Darstellung von $\Phi : \Phi(x) = xT$ mit der Umkehrung $\Phi^{-1}(y) = yT^{-1}$.

Eine **lineare Substitution** $\chi : \mathbb{Z}_N^n \to \mathbb{Z}_N^n$ ist nun aufgebaut als Summe aus einem **homogenen Anteil**, dargestellt durch eine reguläre Matrix $T \in \mathbb{Z}_N^{n,n}$ und einer (polygraphischen) **CAESAR-Addition**, dargestellt durch einen Vektor $t \in \mathbb{Z}_N^n$:

$$\chi(x) = xT + t\ .$$

Beispiel:

Über $\mathbb{Z}_{26}$ seien gegeben eine Matrix T und ein Vektor t ,

$$T \;=\; \begin{pmatrix} 15 & 2 & 7 \\ 8 & 10 & 23 \\ 0 & 2 & 8 \end{pmatrix} \qquad\qquad t \;=\; (\,17 \quad 4 \quad 20\,)$$

Eine $3{\times}3$-Matrix T und ein 3-Vektor t definieren eine tripartite Trigrammsubstitution. Das Bild des Trigramms /mai/ $\hat{=}$ $(\,12 \quad 0 \quad 8\,)$ ergibt sich durch Rechnung *modulo* 26:

$$(\,12 \quad 0 \quad 8\,)\begin{pmatrix} 15 & 2 & 7 \\ 8 & 10 & 23 \\ 0 & 2 & 8 \end{pmatrix} + (\,17 \quad 4 \quad 20\,)$$

$$\stackrel{26}{\simeq} (\,24 \quad 14 \quad 18\,) + (\,17 \quad 4 \quad 20\,) \stackrel{26}{\simeq} (\,15 \quad 18 \quad 12\,) \;\hat{=}\; /\mathrm{psm}/\ .$$

Aber auch das Bild des Trigramms /ecg/ $\hat{=}$ $(\,4 \quad 2 \quad 6\,)$ ist /psm/ , denn auch

$$(\,4 \quad 2 \quad 6\,)\begin{pmatrix} 15 & 2 & 7 \\ 8 & 10 & 23 \\ 0 & 2 & 8 \end{pmatrix} \stackrel{26}{\simeq} (\,24 \quad 14 \quad 18\,)\ .$$

Die Chiffrierung durch die gegebene Matrix T ist also nicht injektiv, T ist nicht regulär und hat keine Inverse. Der Vektor $(8 \ \ -2 \quad 2)$ annulliert T .

5.1 Involutorische lineare Substitutionen

Die Frage liegt nahe: Wann ist eine lineare Substitution χ involutorisch? Die Bedingung lautet, daß $\chi(x) = xT + t = \chi^{-1}(x)$, also

$$x = \chi(\chi(x)) = (xT + t)T + t = xT^2 + tT + t \text{ , woraus}$$

$$T^2 = I \quad \text{und} \quad tT + t = 0$$

folgen. Somit muß die Matrix T des homogenen Anteils involutorisch sein, weswegen als Eigenwerte von T nur 1 oder $N-1$ auftreten können, und der Vektor t muß, wenn er nicht verschwindet, Eigenlösung von T zum Eigenwert $N-1$ sein. Speziell kann χ eine **Spiegelung** sein mit einer Spiegelebene, die als Normale v hat:

$$\chi(x) = x + (1-\gamma(x))\, v \quad \text{mit} \quad v \neq 0$$

wobei das lineare Funktional γ der Bedingung $\gamma(v) = 2$ genügt (im Falle $N = 2$ der Bedingung $\gamma(v) = 0$). Dann gilt $\chi(v) = 0$ und $\chi(0) = v$. Daß $\chi^2(x) = x$, bestätigt man durch Einsetzen:

$$\begin{aligned}\chi(\chi(x)) &= \chi(x) + [1-\gamma(\chi(x))]\, v \\ &= x + (1-\gamma(x))\, v + [1-\gamma(x) - (1-\gamma(x))\gamma(v)]\, v \\ &= x + (1-\gamma(x))v + [\ (1-\gamma(x)) - 2(1-\gamma(x))\ ]\, v \ = \ x \ .\end{aligned}$$

Beispiel: $\mathbb{Z}_2^2 \to \mathbb{Z}_2^2$ ($n=2$, d.h. zweikomponentige Zeilenvektoren, $N=2$)

$$\chi((x_1 \;\; x_2)) = (x_1 \;\; x_2) + (1-x_1-x_2)\,(1 \;\; 1) = (1-x_2 \;\; 1-x_1) =$$

$$(x_1 \;\; x_2)\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} + (1 \;\; 1) \ .$$

$$\begin{aligned}\chi((0\ 0)) &= (1\ 1)\\ \chi((0\ 1)) &= (0\ 1)\\ \chi((1\ 0)) &= (1\ 0)\\ \chi((1\ 1)) &= (0\ 0)\end{aligned}$$

(0 1) (1 1)
(0 0) (1 0)

Der Klartext 001001110110110001 wird chiffriert in den Geheimtext 111001000110001101 und umgekehrt.

5.2 Homogene und inhomogene lineare Substitutionen

5.2.1 Wir betrachten zunächst den Spezialfall der **homogenen linearen** (‚affinen') **Substitution**, $t = 0$ (HILL-Chiffrierschritt).

Nachfolgend ein Beispiel über $\mathbb{Z}$ für eine reguläre (quadratische) Matrix der Determinante $+1$ mit $n = 4$ und ihre Inverse:

$$T = \begin{pmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{pmatrix} \qquad T^{-1} = \begin{pmatrix} -3 & 20 & -21 & 1 \\ 2 & -41 & 44 & 1 \\ 2 & -6 & 6 & -1 \\ -1 & 28 & -30 & -1 \end{pmatrix} .$$

Bei der Zahlenrechnung spart man sich Rechenarbeit, wenn man auch kleine negative Zahlen als Repräsentanten der Restklassen benutzt, über $\mathbb{Z}_{26}$ neben

$$T^{-1} \overset{26}{\simeq} \begin{pmatrix} 23 & 20 & 5 & 1 \\ 2 & 11 & 18 & 1 \\ 2 & 20 & 6 & 25 \\ 25 & 2 & 22 & 25 \end{pmatrix} \quad \text{auch} \quad T^{-1} \overset{26}{\simeq} \begin{pmatrix} -3 & -6 & 5 & 1 \\ 2 & 11 & -8 & 1 \\ 2 & -6 & 6 & -1 \\ -1 & 2 & -4 & -1 \end{pmatrix} .$$

Beispiel: Das Bild des Tetragramms /ende/ $\hat{=}$ $(4 \;\; 13 \;\; 3 \;\; 4)$ ergibt sich durch Rechnung *modulo* 26 zu /jhbl/ $\hat{=}$ $(9 \;\; 7 \;\; 1 \;\; 11)$:

$$(4 \;\; 13 \;\; 3 \;\; 4) \begin{pmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{pmatrix} \overset{26}{\simeq} (9 \;\; 7 \;\; 1 \;\; 11) ,$$

$$(9 \;\; 7 \;\; 1 \;\; 11) \begin{pmatrix} 23 & 20 & 5 & 1 \\ 2 & 11 & 18 & 1 \\ 2 & 20 & 6 & 25 \\ 25 & 2 & 22 & 25 \end{pmatrix} \overset{26}{\simeq} (4 \;\; 13 \;\; 3 \;\; 4) .$$

5.2.2 Mit $t = (3 \;\; 8 \;\; 5 \;\; 20)$ und T wie oben ist eine **inhomogene lineare** (‚affine') **Substitution** χ gegeben

$$\chi(x_1 \; x_2 \; x_3 \; x_4) = (x_1 \; x_2 \; x_3 \; x_4) \begin{pmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{pmatrix} + (3 \;\; 8 \;\; 5 \;\; 20)$$

mit der Umkehrung

$$\chi^{-1}(y_1 \; y_2 \; y_3 \; y_4) = (y_1 \; y_2 \; y_3 \; y_4) \begin{pmatrix} 23 & 20 & 5 & 1 \\ 2 & 11 & 18 & 1 \\ 2 & 20 & 6 & 25 \\ 25 & 2 & 22 & 25 \end{pmatrix} + (3 \;\; 24 \;\; 21 \;\; 14) .$$

5.2.3 Die Anzahl regulärer n-reihiger Matrizes über $\mathbb{Z}_N$ hängt von der Primalität von N ab. Bekannt ist[2]

Satz. Sei $N = p$, p prim. Die Anzahl $g(p, n)$ regulärer Matrizes aus $\mathbb{Z}_p^{n,n}$ ist

$$g(p, n) = (p^n - 1)\,(p^n - p)\,(p^n - p^2) \,.\,.\, (p^n - p^{n-1}) \quad .$$

Die Anzahl verschiedener Matrizes überhaupt ist p^{n^2}. Es gilt

$$g(p, n) = p^{n^2} \cdot \rho(p, n) \quad ,$$

wo

$$\rho(p, n) = \prod_{k=1}^{n} (1 - \frac{1}{p^k}) \quad .$$

Für den binären Fall $N{=}2$: $g(2,1) = 1$, $g(2,2) = 2^1 \cdot 3$, $g(2,3) = 2^3 \cdot 3 \cdot 7$, $g(2,4) = 2^6 \cdot 3 \cdot 7 \cdot 15$, $g(2,5) = 2^{10} \cdot 3 \cdot 7 \cdot 15 \cdot 31$, $g(2,6) = 2^{15} \cdot 3 \cdot 7 \cdot 15 \cdot 31 \cdot 63$.

[2] siehe *Heinz-Richard Halder, Werner Heise*: Einführung in die Kombinatorik, S. 206.

Dabei ist (*Euler* 1760)

$$\lim_{n\to\infty} \rho(p,\,n) = h(\tfrac{1}{p})\ , \qquad \text{wo}$$

$$h(x) = 1 + \sum_{k=1}^{\infty} (-1)^k \left[x^{(3k^2-k)/2} + x^{(3k^2+k)/2}\right]$$
$$= 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} \ldots$$

eine lakunäre Reihe ist, die mit Thetareihen[3] zusammenhängt. $h(\frac{1}{p})$ liefert für größere n eine gute Abschätzung für $\rho(p,\,n)$; einige Werte für Primzahlen p sind

$N=p$	$h(\frac{1}{p})$	$\ln h(\frac{1}{p})$
2	0.28879	−1.24206
3	0.56013	−0.57959
5	0.76033	−0.27400
7	0.83680	−0.17817
11	0.90083	−0.10444
13	0.91716	−0.08647
17	0.93772	−0.06430
19	0.94460	−0.05699

Für $p > 10$ gibt $1 - \frac{1}{p} - \frac{1}{p^2}$ bereits 5 genaue Stellen für $h(\frac{1}{p})$;
$1/(\frac{3}{2} - p)$ nähert $\ln h(\frac{1}{p})$ mit einem relativen Fehler kleiner als $\frac{1}{p^2}$.

Die Anzahl *involutorischer* Matrizen ist größenordnungsmäßig $\sqrt{g(p,n)}$.

Für Primzahlpotenzen gelangt man auf folgende Weise weiter:

Satz (*Manfred Broy*, 1981)

Sei N Primzahlpotenz, $N = p^s$ und $A \in \mathbb{Z}_N^{n,n}$. Dann existieren $A_i \in \mathbb{Z}_p^{n,n}$, $0 \leq i < s$ derart, daß A in der Form $A = \sum_{i=0}^{s-1} A_i\, p^i$ eindeutig darstellbar ist. A ist regulär genau dann, wenn A_0 regulär ist.

Daraus folgt

$$g(p^s,\,n) = g(p,\,n)\cdot\left(p^{n^2}\right)^{s-1} = \left(p^{n^2}\right)^s\cdot\rho(p,\,n) = (p^s)^{n^2}\cdot\rho(p,\,n) = N^{n^2}\cdot\rho(p,\,n)\ .$$

Schließlich ergibt sich, wenn $N = p_1^{s_1}\cdot p_2^{s_2}\ldots p_k^{s_k}$, als Anzahl regulärer Matrizen

$$g(N,\ n) = N^{n^2}\cdot\rho(p_1,\,n)\cdot\rho(p_2,\,n)\ \cdot\ \ldots\ \rho(p_k,\,n)\ .$$

Verglichen mit der Anzahl $(N^n)!$ *aller* polygraphischen Substitutionen ist das nicht viel: für $N = 25$, $n = 4$ ist $(N^n)! \approx 10^{2\,184\,284}$, demgegenüber beträgt $N^{n^2} = 2.33\cdot 10^{22}$ und $g(N,\ n) = 1.77\cdot 10^{22}$. Das reicht knapp an die Anzahl $6.20\cdot 10^{23}$ einfacher zyklischer Permutationen für $N = 25$ heran.

Für $N = 25$ ist $g(25,1) = 20$, $g(25,2) = 300\,000$, $g(25,3) = 2\,906\,250\,000\,000$;
für $N = 26$ ist $g(26,1) = 12$, $g(26,2) = 157\,248$, $g(26,3) = 1\,634\,038\,189\,056$.

---

[3] Siehe etwa *R. Remmert*, Funktionentheorie I, Springer 1984, S. 263.

5.2.4 Die Konstruktion einer regulären Matrix geschieht am einfachsten als Produkt einer unteren mit einer oberen regulären Dreiecksmatrix. Dazu müssen die Diagonalelemente invertierbar sein (s. 5.5, Tabelle 1), am einfachsten nimmt man Einsen in die Diagonale. Außerdem kann man die obere Dreiecksmatrix als transponierte der unteren wählen, dadurch erhält man symmetrische Matrizes. Die Invertierung der Dreiecksmatrizes zwecks Erzielung der inversen Abbildung geschieht nach der Eliminationsmethode. Es ist auch möglich, diese Rechnung zuerst in $\mathbb{Z}$ auszuführen und dann zu den Restklassen überzugehen.

Beispiel

$$\begin{pmatrix} 1 & & \\ 3 & 1 & \\ 5 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & 5 \\ & 1 & 2 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 \\ 3 & 10 & 17 \\ 5 & 17 & 30 \end{pmatrix} ;$$

$$\begin{pmatrix} 1 & & \\ 3 & 1 & \\ 5 & 2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & & \\ -3 & 1 & \\ 1 & -2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 5 \\ & 1 & 2 \\ & & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -3 & 1 \\ & 1 & -2 \\ & & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & -3 & 1 \\ & 1 & -2 \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & & \\ -3 & 1 & \\ 1 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 11 & -5 & 1 \\ -5 & 5 & -2 \\ 1 & -2 & 1 \end{pmatrix} .$$

Für $\mathbb{Z}_{26}$ bzw. $\mathbb{Z}_{25}$ sind somit

$$\begin{pmatrix} 1 & 3 & 5 \\ 3 & 10 & 17 \\ 5 & 17 & 4 \end{pmatrix}, \begin{pmatrix} 11 & 21 & 1 \\ 21 & 5 & 24 \\ 1 & 24 & 1 \end{pmatrix} \quad \text{bzw.} \quad \begin{pmatrix} 1 & 3 & 5 \\ 3 & 10 & 17 \\ 5 & 17 & 5 \end{pmatrix}, \begin{pmatrix} 11 & 20 & 1 \\ 20 & 5 & 23 \\ 1 & 23 & 1 \end{pmatrix}$$

ein Paar (symmetrischer) inverser Matrizes, für $\mathbb{Z}_{10}$ bzw. $\mathbb{Z}_2$ sind es

$$\begin{pmatrix} 1 & 3 & 5 \\ 3 & 0 & 7 \\ 5 & 7 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 5 & 1 \\ 5 & 5 & 8 \\ 1 & 8 & 1 \end{pmatrix} \quad \text{bzw.} \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} .$$

Wählt man für gegebenes n und N die untere Dreiecksmatrix L wie auch die obere Dreiecksmatrix U (mit Einsen in der Diagonale) ganz beliebig und für D eine Diagonalmatrix mit invertierbaren Elementen, so erhält man bis auf Umordnung von Zeilen und Spalten alle Paare gegenseitig inverser Matrizes LDU und $U^{-1}D^{-1}L^{-1}$.

5.2.5 Die Konstruktion einer involutorischen Matrix ist kaum schwieriger: Ist für gegebenes n und N $(X\ ,\ X^{-1})$ ein Paar gegenseitig inverser Matrizes und ist J eine involutorische Diagonalmatrix, deren Elemente $+1$ oder -1 (allgemeiner: in $\mathbb{Z}_N$ zu sich selbst reziprok) sind, so ist $X\,J\,X^{-1}$ involutorisch.

Beispiel

$$\begin{pmatrix} 1 & 3 & 5 \\ 3 & 10 & 17 \\ 5 & 17 & 30 \end{pmatrix} \begin{pmatrix} 1 & & \\ & -1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} 11 & -5 & 1 \\ -5 & 5 & -2 \\ 1 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 31 & -30 & 12 \\ 100 & -99 & 40 \\ 170 & -190 & 69 \end{pmatrix} .$$

Für $\mathbb{Z}_{26}$, $\mathbb{Z}_{25}$, $\mathbb{Z}_{10}$, $\mathbb{Z}_2$ ergeben sich somit die involutorischen Matrizes

$$\begin{pmatrix} 5 & 22 & 12 \\ 22 & 3 & 14 \\ 14 & 18 & 17 \end{pmatrix} , \begin{pmatrix} 6 & 20 & 12 \\ 0 & 1 & 15 \\ 20 & 5 & 19 \end{pmatrix} , \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 9 \end{pmatrix} , \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

Über $\mathbb{Z}_2$ ist die Identität die einzige involutorische Diagonalmatrix.

Für die Anzahl involutorischer n-reihiger Matrizes über $\mathbb{Z}_N$ ist keine einfache Formel bekannt.

5.3 Binäre lineare Substitutionen

Für $\mathbb{Z}_2$, d.h. für Binärwörter (der Länge n_0) des Klar- und des Geheimtextes, wird die technische Durchführung von linearen Substitutionen besonders einfach. Die Arithmetik *modulo* 2 läßt sich in Boolesche Algebra übersetzen und mit binären Schaltungen der Breite n_0 realisieren, für nicht zu großes n_0 sogar parallel.

Vergleicht man den Fall $\mathbb{Z}_{2^s}^{n_0 \times n_0} (n = n_0, N = 2^s)$ mit dem Fall $\mathbb{Z}_2^{s \cdot n_0 \times s \cdot n_0}$ $(n = s \cdot n_0 , N = 2)$ der sich ergibt, wenn man die 2^s Zeichen von $\mathbb{Z}_{2^s}^{n_0 \times n_0}$ in Binärwörter der Länge s auflöst, so beträgt die Anzahl aller linearen Substitutionen $2^{s \cdot n_0^2} \cdot \rho(2, n_0) = K \cdot \rho(2, n_0)$ im ersteren Fall, $2^{s^2 \cdot n_0^2} \cdot \rho(2, s \cdot n_0) = K^s \cdot \rho(2, s \cdot n_0)$ im letzteren Fall. Die feinere Auflösung, die $\mathbb{Z}_2$ vornimmt, erhöht also die Mächtigkeit der Verfahrensklasse der linearen Substitutionen.

5.4 Allgemeine lineare Substitutionen

Nimmt man noch die N^n CAESAR-Additionen hinzu, so hat man von der Größenordnung N^{n^2+n} lineare Substitutionen insgesamt. Selbstreziproke homogene lineare Substitutionen (mit $N = 26$) hat 1929 *Lester S. Hill*[4] vorgeschlagen, ein Vorläufer ist *F. J. Buck* (1772)[5]. *Hills* Ideen wurden 1941 von *A. A. Albert* in einer Woge patriotischer wie mathematischer Begeisterung aufgegriffen, insbesondere in einem Vortrag auf einem Treffen der American

---

[4] *Lester S. Hill* war damals, 38 Jahre alt, *assistant professor of mathematics* am Hunter College in New York. Er hatte 1926 in Yale seinen Doktor gemacht, nachdem er an verschiedenen Colleges Lehrer gewesen war. Die Arbeit ist in *The American Mathematical Monthly* unter dem Titel "Cryptography in an Algebraic Alphabet" erschienen (Band **36**, S. 306–312, Juni–Juli 1929), sowie eine Nachfolgearbeit "Concerning certain linear transformation apparatus of cryptography" (Band **37**, S. 135–154, März 1931). *Hill* blieb bis 1960 Professor am Hunter College, er starb am 9. Januar 1961.

[5] *L. J. d'Auriol* verwendete 1867 eine Bigrammverschlüsselung $V^2 \to V^2$, die möglicherweise eine spezielle lineare Substitution ist.

Mathematical Society. Zu diesem Zeitpunkt hatten sie aber bereits ihre Auswirkungen gehabt, auf *W. F. Friedman* in den Staaten, auf *Werner Kunze* im Auswärtigen Amt.[6] *Hill*s Bedeutung liegt vor allem darin, daß seither der Wert mathematischer Methoden in der Kryptologie unumstritten ist. So ist es nur konsequent, daß in den dreißiger Jahren Mathematiker in die Chiffrierbüros einzogen, *Solomon Kullback* (1907–1994), *Abraham Sinkov* (∗ 1907), *Werner Kunze*, *Maurits de Vries* und viele, deren Namen verborgen bleiben.

Lester S. Hill konstruierte auch eine Maschine, die (für $n = 6$) lineare Substitutionen durchführte, und bekam dafür ein Patent (U.S. Patent 1.845,947). Ein rein mechanisches Gerät mit Zahnrädern befriedigte aber nicht sehr, und so wurde *Hill*s Erfindung im 2. Weltkrieg nur benutzt, um 3-Buchstaben-Gruppen von Radio-Rufzeichen zu verschlüsseln – gegenüber der Berechnung von Hand bereits ein beträchtlicher Gewinn.

5.5 Zerfallende lineare Substitutionen

Als Spezialfall steckt hinter der linearen Substitution jedoch auch eine spezielle poly*alphabetische* Chiffrierung. Dies ist so, wenn T in direkte Bestandteile zerfällt, $T = T_1 \oplus T_2 \oplus \cdots \oplus T_r$, also blockdiagonal ist,

$$T = \left(\begin{array}{c|c|c|c} T_1 & 0 & \dots & 0 \\ \hline 0 & T_2 & \dots & 0 \\ \hline \vdots & \vdots & \dots & 0 \\ \hline 0 & 0 & 0 & T_r \end{array}\right)$$

wobei T_i n_i-reihig ist. Dann definiert jedes T_i , zusammen mit dem entsprechenden Anteil t_i von $t = t_1 \oplus t_2 \oplus \cdots \oplus t_r$, eine polygraphische Substitution, eine Chiffrierung von n_i-grammen. Sofern diese r Substitutionen paarweise verschieden sind, handelt es sich gleichzeitig um eine r-fach polyalphabetische, lineare polygraphische Chiffrierung. Mehr darüber in 7.4.1 .

Ein wichtiger Extremfall ist $n_i = 1$, $r = n$. Dann ist T eine Diagonalmatrix, in jeder Zeile liegt eine **einfache lineare** (‚affine') **Substitution**, eine spezielle unipartite monographische Substitution $T_i : V^1 \rightarrow V^1$ vor.

---

[6] Dr. *Werner Kunze*, geboren etwa 1890, hatte in Heidelberg Mathematik, Physik und Philosophie studiert, war Kavallerist im 1. Weltkrieg und kam im Januar 1918 zur Kryptologie im AA. Er brach 1923 einen überschlüsselten diplomatischen Code Frankreichs, 1936 ORANGE und später RED, zwei japanische Rotor-Schlüsselmaschinen. *Kunze* war vermutlich der erste professionelle Mathematiker, der in einem modernen kryptanalytischen Büro beschäftigt war. *Kunze* war, gleich *Mauborgne*, ein passabler Violinspieler, auch *Strachey* wurde als guter Musiker gerühmt, während *Painvin* ein ausgezeichneter Cellist war. *Lambros D. Callimahos*, N.S.A., war ein berühmter Flötist.

N=2	1									$\mathcal{M}_2 = \mathcal{C}_1$
N=3	1	**2**								$\mathcal{M}_3 = \mathcal{C}_2$
N=4	1	**3**								$\mathcal{M}_4 = \mathcal{C}_2$
N=5	1	**2** 3	4							$\mathcal{M}_5 = \mathcal{C}_4$
N=6	1	**5**								$\mathcal{M}_5 = \mathcal{C}_2$
N=7	1	2 4	**3** 5	6						$\mathcal{M}_7 = \mathcal{C}_6$
N=8	1	**3**	5	**7**						$\mathcal{M}_8 = \mathcal{C}_2 \times \mathcal{C}_2$
N=9	1	**2** 5	4 7	8						$\mathcal{M}_9 = \mathcal{C}_6$
N=10	1	**3** 7	9							$\mathcal{M}_{10} = \mathcal{C}_4$
N=11	1	**2** 6	3 4	5 9	7 8	10				$\mathcal{M}_{11} = \mathcal{C}_{10}$
N=12	1	**5**	7	**11**						$\mathcal{M}_{12} = \mathcal{C}_2 \times \mathcal{C}_2$
N=13	1	**2** 7	3 9	4 10	5 8	6 11	12			$\mathcal{M}_{13} = \mathcal{C}_{12}$
N=14	1	**3** 5	9 11	13						$\mathcal{M}_{14} = \mathcal{C}_6$
N=15	1	**2** 8	4	7 13	11	**14**				$\mathcal{M}_{15} = \mathcal{C}_4 \times \mathcal{C}_2$
N=16	1	**3** 11	5 13	7	9	**15**				$\mathcal{M}_{16} = \mathcal{C}_4 \times \mathcal{C}_2$
N=17	1	2 9	**3** 6	4 13	5 7	8 15	10 12	11 14	16	$\mathcal{M}_{17} = \mathcal{C}_{16}$

Tabelle 1 a. Selbstreziproke Elemente und reziproke Paare in $\mathbb{Z}_N$ für N von 2 bis 17 (Fettgedruckt ist jeweils ein Satz erzeugender Elemente der multiplikativen Gruppe $\mathcal{M}_N$)

N=18	1 **5**/11 7/13 17	$\mathcal{M}_{18} = \mathcal{C}_6$
N=19	1 **2**/10 3/13 4/5 6/16 7/11 8/12 9/17 14/15 18	$\mathcal{M}_{19} = \mathcal{C}_{18}$
N=20	1 **3**/7 9 11 13/17 **19**	$\mathcal{M}_{20} = \mathcal{C}_4 \times \mathcal{C}_2$
N=21	1 **2**/11 4/16 5/17 8 10/19 13 **20**	$\mathcal{M}_{21} = \mathcal{C}_6 \times \mathcal{C}_2$
N=22	1 3/15 5/9 **7**/19 13/17 21	$\mathcal{M}_{22} = \mathcal{C}_{10}$
N=23	1 2/12 3/8 4/6 **5**/14 7/10 9/18 11/21 13/16 15/20 17/19 22	$\mathcal{M}_{23} = \mathcal{C}_{22}$
N=24	1 **5** 7 11 **13** 17 19 **23**	$\mathcal{M}_{24} = \mathcal{C}_2 \times \mathcal{C}_2 \times \mathcal{C}_2$
N=25	1 **2**/13 3/17 4/19 6/21 7/18 8/22 9/14 11/16 12/23 24	$\mathcal{M}_{25} = \mathcal{C}_{20}$
N=26	1 3/9 5/21 **7**/15 11/19 17/23 25	$\mathcal{M}_{26} = \mathcal{C}_{12}$
N=27	1 **2**/14 4/7 5/11 8/17 10/19 13/25 16/22 20/23 26	$\mathcal{M}_{27} = \mathcal{C}_{18}$
N=28	1 **3**/19 5/17 9/25 11/23 13 15 **27**	$\mathcal{M}_{28} = \mathcal{C}_6 \times \mathcal{C}_2$
N=29	1 **2**/15 3/10 4/22 5/6 7/25 8/11 9/13 12/17 14/27 16/20 18/21 19/26 23/24 28	$\mathcal{M}_{29} = \mathcal{C}_{28}$
N=30	1 **7**/13 11 17/23 19 **29**	$\mathcal{M}_{30} = \mathcal{C}_4 \times \mathcal{C}_2$
N=31	1 2/16 **3**/21 4/8 5/25 6/26 7/9 10/28 11/17 12/13 14/20 15/29 18/19 22/24 23/27 30	$\mathcal{M}_{31} = \mathcal{C}_{30}$
N=32	1 **3**/11 5/13 7/23 9/25 15 17 19/27 21/29 **31**	$\mathcal{M}_{32} = \mathcal{C}_8 \times \mathcal{C}_2$
N=33	1 **2**/17 4/25 5/20 7/19 8/29 10 13/28 14/26 16/31 23 **32**	$\mathcal{M}_{33} = \mathcal{C}_{10} \times \mathcal{C}_2$

Tabelle 1 b. Selbstreziproke Elemente und reziproke Paare in $\mathbb{Z}_N$ für N von 18 bis 33 (Fettgedruckt ist jeweils ein Satz erzeugender Elemente der multiplikativen Gruppe $\mathcal{M}_N$)

Betrachten wir diesen monographischen Fall — eine Permutation. Es ist $\chi(x) = q \cdot x + t$ sicher regulär für $q = 1$, $\chi(x) = x + t$ mit der Umkehrung $\chi^{-1}(x) = x - t$. Dies liefert für $t \neq 0$ eine CAESAR-Addition. Für $\chi(x) = x+i$ schreiben wir hinfort auch $\chi(x) = \rho^i(x)$, wo $\rho(x) = x+1$. Allgemein gilt

$\chi(x) = q \cdot x + t$ ist regulär genau dann, wenn q teilerfremd ist zu N .

Tabelle 1 gibt für einige gebräuchliche Werte von N selbstreziproke q und reziproke Paare von q und q^{-1} , sowie die Darstellung der multiplikativen Gruppen $\mathcal{M}_N$ als Produkte zyklischer Gruppen $\mathcal{C}_i$ von i Elementen.

5.6 Dezimierte Alphabete

Der homogene Fall liefert neben den Trivialfällen involutorischer Alphabete
$q = q^{-1} = 1$ (unverändertes Alphabet) und
$q = q^{-1} = N-1$ (**komplementäres Alphabet**)
die **dezimiertenen Alphabete** (frz. *alphabets chevauchants*), die *Eyraud* betrachtet: Alphabete, die man erhält, wenn man für $q > 1$ als Repräsentanten die q-fachen *modulo N* (*Sinkov*: *'decimation by q'*) nimmt. *Eyraud* gibt auch die Bedingung der Teilerfremdheit von q und N an.

Beispiele für $N = 8$:

$$q = 1 : \begin{pmatrix} a & b & c & d & e & f & g & h \\ a & b & c & d & e & f & g & h \end{pmatrix} = (a)\,(b)\,(c)\,(d)\,(e)\,(f)\,(g)\,(h)$$

$$q = 7 : \begin{pmatrix} a & b & c & d & e & f & g & h \\ a & h & g & f & e & d & c & b \end{pmatrix} = (a)\,(bh)\,(cg)\,(df)\,(e)$$

$$q = 3 : \begin{pmatrix} a & b & c & d & e & f & g & h \\ a & d & g & b & e & h & c & f \end{pmatrix} = (a)\,(bd)\,(cg)\,(e)\,(fh)$$

$$q = 5 : \begin{pmatrix} a & b & c & d & e & f & g & h \\ a & f & c & h & e & b & g & d \end{pmatrix} = (a)\,(bf)\,(c)\,(dh)\,(e)\,(g) \quad .$$

Das komplementäre Alphabet ergibt sich mit der Abbildung

$$\chi(x) = (N-1) \cdot x \quad \stackrel{N}{\simeq} \quad N - x \quad \stackrel{N}{\simeq} \quad -x \, .$$

Das **revertierte Alphabet** ergibt sich aus dem inhomogenen Fall mit der Abbildung

$$\chi(x) = (N-1) \cdot (x+1) \stackrel{N}{\simeq} (N-1) - x \stackrel{N}{\simeq} -x - 1 \, .$$

Die Anzahl $g(N,1)$ regulärer homogener Abbildungen stimmt mit der Eulerschen Funktion $\varphi(N)$, der Anzahl der zu N teilerfremden Zahlen unter den Zahlen $1, 2, \ldots, N-1$ überein.

Ist $N = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_k^{s_k}$, so ist

$$\begin{aligned}\varphi(N) &= (p_1 - 1) \cdot p^{s_1 - 1} \cdot (p_2 - 1) \cdot p^{s_2 - 1} \cdot \ \ldots \ \cdot (p_k - 1) \cdot p^{s_k - 1} \\ &= N \cdot (1 - \tfrac{1}{p_1}) \cdot (1 - \tfrac{1}{p_2}) \cdot \ \ldots \ \cdot (1 - \tfrac{1}{p_s}) \, .\end{aligned}$$

5.7 Lineare Substitutionen mit Dezimalzahlen und Dualzahlen

Man beachte den Unterschied zwischen $\mathbb{Z}_N^n$, das zu V^n gehört, und $\mathbb{Z}_{N^n}$, auf das man geführt wird, wenn V^n etwa lexikographisch geordnet wird.

5.7.1 Fall $N = 10$: Die dezimierten Alphabete (vgl. 5.6) für n-ziffrige Dezimalzahlen, d.h. für $\mathbb{Z}_{10^n}$, sind besonders interessant für Amateure[7], die in $\mathbb{Z}_{10^n}$ mit einem Taschenrechner chiffrieren, da dieser neben der Addition auch die Multiplikation mit einem festen Faktor q erleichtert.

Beispiel $n = 2$ ($\mathbb{Z}_{100}$): Es genügt, für Primzahlen bis 97 (ohne 2 und 5) die Reziproken *modulo* 100 zu kennen:

h	=	3	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
h^{-1}	=	67	43	91	77	53	79	87	69	71	73	61	7	83	17	39	41	3	31	27	19	47	9	33

Dabei ist die Endziffer der Reziproken schon durch das Reziproke *modulo* 10 der Endziffer bestimmt, vgl. Tabelle 1, $N = 10$. Dies legt für größere Werte von n ein stufenweises Vorgehen nahe: Man bestimmt jeweils eine weitere Ziffer passend.

Beispiel $n = 5$ ($\mathbb{Z}_{10^5}$): Das Reziproke *modulo* 10^5 etwa von $h = 32\,413$ ergibt sich zu $h^{-1} = 3\,477$ mit folgendem Algorithmus

$$\begin{array}{rlll}
3: & & & 7 \cdot 3 = \mathbf{2} \cdot 10 + 1 \\
\mathbf{1}3: & \mathbf{2} + \mathbf{1} \cdot 7 + 3 \cdot x \overset{10}{\simeq} 0 & x = \mathbf{7} & \mathbf{7}7 \cdot 13 = \mathbf{10} \cdot 10^2 + 1 \\
\mathbf{4}13: & \mathbf{10} + \mathbf{4} \cdot 7 + 3 \cdot x \overset{10}{\simeq} 0 & x = \mathbf{4} & \mathbf{4}77 \cdot 413 = \mathbf{197} \cdot 10^3 + 1 \\
\mathbf{2}413: & \mathbf{197} + \mathbf{2} \cdot 7 + 3 \cdot x \overset{10}{\simeq} 0 & x = \mathbf{3} & \mathbf{3}477 \cdot 2413 = \mathbf{839} \cdot 10^4 + 1 \\
\mathbf{3}2413: & \mathbf{839} + \mathbf{3} \cdot 7 + 3 \cdot x \overset{10}{\simeq} 0 & x = \mathbf{0} & \mathbf{0}3477 \cdot 32413 = \mathbf{1127} \cdot 10^5 + 1
\end{array}$$

Der Aufwand zur Bestimmung der Reziproken einer n-stelligen Zahl geht proportional n^2.

5.7.2 Fall $N = 2$: Für professionelles Arbeiten ist das Dualsystem vorzuziehen. Die Fälle $n = 8, 16, 32$ oder gar 64 passen direkt auf die Internarithmetik von Mikroprozessoren dieser Verarbeitungsbreiten. Der Algorithmus zur Bestimmung einer Reziproken *modulo* 2^n verläuft analog dem obigen, ist überdies wie der klassische Dualalgorithmus der Division noch einfacher als der für den Fall *modulo* 10^n.

Beispielsweise erhält man zu **LOOO OOOO OOLL OLLL** = 32823
reziprok *modulo* 2^{16} **OOLL OLOL LOOO OLLL** = 13703

In der Tat ist $32823 \cdot 13703 = 449773569 = 1 + 6863 \cdot 2^{16}$.

5.7.3 *Alan Turing* machte sich bereits 1937, zwei Jahre bevor er ernsthaft mit Kryptanalyse befaßt war, Gedanken über eine Chiffrierung durch Multiplikation im Dualsystem. Das mag manchem Mathematiker gelegentlich vorgeschwebt haben; *Turing* entwarf jedoch eine Relais-Multiplikationsschaltung

[7] Auch mit einem mechanischen Addiergerät kann man leicht in $\mathbb{Z}_{10^n}$ rechnen. Um zum Rechnen in $\mathbb{Z}_{10}^n$ überzugehen, muß man die Übertragseinrichtung ausbauen (vgl. 8.3.3).

dafür und baute auch die ersten Stufen, mit Unterstützung durch den Physiker *Malcolm McPhail*. Die Umstände veranlaßten *Turing*, als er im Juli 1938 aus Princeton zurückgekehrt war, dieses Vorhaben nicht weiter zu verfolgen – aber er war darauf vorbereitet, die maschinelle Kryptanalyse in Angriff zu nehmen, als er am 4. September 1939, einen Tag nach Kriegsausbruch, in *Bletchley Park*, einem Schlößchen in Buckinghamshire, auf halbem Weg zwischen Oxford und Cambridge, einzog. Die dorthin im August 1939 verlagerte *Government Code and Cypher School* hatte mit ihm schon im Sommer 1938 Kontakt aufgenommen, dabei war er mit dem in erster Linie um die ENIGMA-Entzifferung bemühten *Dillwyn Knox* zusammengetroffen.[8]

Auch *Gordon Welchman* wurde für die *Government Code and Cypher School* vor Kriegsausbruch rekrutiert. Der erste Mathematiker, der dort regulären Dienst machte, war jedoch *Peter Twinn*, ein Mann aus Oxford, der im Februar 1939 anfing. Ihm wurde später verraten, daß man einige Zweifel hatte, ob es weise war, einen Mathematiker anzuheuern, “as they were regarded as strange fellows notoriously unpractical” (*Christopher Andrew*). Tatsächlich hatten einige andere frühe Mitstreiter, wie *Gordon Welchman* und *Dennis Babbage* wenigstens einige Erfahrungen im Schachspiel, nicht zu reden von den Schachmeistern *Stuart Milner-Barry*, *Harry Golombek* und *Hugh Alexander*, die alle von *Welchman* angeworben wurden.



Gordon Welchman (1906–1985)

Großbritannien war auf den heraufziehenden Krieg gut vorbereitet; aus Oxford und Cambridge kamen die besten Leute, wenn sie nicht Jagdflieger werden wollten, nach *Bletchley Park*. Seit Mitte 1938 war man in der GC&CS alarmiert. Weder die Vereinigten Staaten noch Deutschland trafen solch minuziöse Vorkehrungen in der Rekrutierung von Wissenschaftlern. In Großbritannien hatte man später als in den U.S.A. oder in Deutschland die Bedeutung der Mathematik für die Kryptanalyse erkannt, mit *Turing* und *Welchman* holte man jedoch gründlich auf. Die Talente unkonventioneller und exzentrischer Persönlichkeiten ausbeutend, war das britische *Foreign Office* in der Lage, das fähigste Team von Kryptanalysten in der britischen Geschichte zusammenzubringen. In Frankreich, dessen Kryptologie wie die britische extrem linguistisch orientiert war, bot sich dazu keine Gelegenheit mehr, nachdem es 1940 überrannt worden war.

---

[8] Es ist zweifelhaft, ob man *Cave Brown* glauben darf, daß Mitte 1938 *Knox* und *Turing* nach Warschau reisten, um durch Vermittlung des polnischen Geheimdienstes einen Polen mit Pseudonym *Lewinski* zu treffen, der angeblich bei *Heimsoeth & Rincke* in Berlin als Mathematiker und Ingenieur gearbeitet hatte und sich erbot, einen Nachbau der ENIGMA zu besorgen.
Jedoch berichtet auch *Harry Hinsley*, daß bereits 1938 der polnische Geheimdienst in Sachen ENIGMA Fühler zur GC&CS und zu *Knox* ausgestreckt hatte. *Knox* beklagte sich seinerseits, als er zu diesem frühen Zeitpunkt mit leeren Händen zurückkam, die Polen “were stupid and knew nothing”.

6 Chiffrierschritte: Transposition

«En un mot, les méthodes de transposition sont une salade des lettres du texte clair.»
Étienne Bazeries

Ein im 5. Kapitel gar nicht behandelter extremer Spezialfall einer homogenen linearen Substitution stützt sich auf reguläre Matrizes, die nur mit 0 und 1 besetzt sind, was für $N > 2$ eine echte, und zwar schwere Einschränkung bedeutet.

Verlangt man überdies, daß in jeder Zeile und in jeder Spalte genau einmal 1 und sonst 0 vorkommt, so bekommt man eine Permutationsmatrix; die lineare Substitution bewirkt eine bloße Permutation der Basis.

Die **Transposition** (engl. *transposition*, deutsch auch ‚Umstellung', ‚Würfelverfahren'[1] oder ‚Versatzverfahren') ist also eine polygraphische Substitution π aus $\gamma_n : V^n \to V^n$, eine *Codierung* speziellster Art

$$(x_1\ ,\ x_2\ ,\ \ldots\ x_n)\ \mapsto\ (x_{\pi(1)}\ ,\ x_{\pi(2)}\ ,\ \ldots\ x_{\pi(n)})$$

wo π eine Permutation von $\{1 \ldots n\}$ ist. Sie wechselt nicht Alphabetzeichen aus, sondern permutiert Plätze. Uralt ist ihre Verwendung für **Anagramme** (Bolivia - Lobivia), insbesondere zur Bildung von Pseudonymen.[2]

6.1 Einfachste Verfahren

Die einfachsten Verfahrensklassen sind einelementig oder haben nur geringen Umfang.

6.1.1 Krebs: Wortweise oder im ganzen die Nachricht rückwärts gelesen.

Beispiele: Lirpa Occabot Kool , vgl. auch 1.4.

Hierunter fallen auch **Ananyme** wie ‚Remarque' für ‚Kramer', ‚Ave' für ‚Eva'. Krebs ist auch eine in der Musik bekannte Chiffrierung: Krebskanon.

Palindrome[3] sind Wörter oder Sätze, die unter Krebs invariant sind:

---

[1] Eigentlich ‚Verwerfung', vgl. den Gebrauch des Wortes ‚Gleis-Verwerfung' für eine Permutation von Eisenbahngeleisen.

[2] Anagramme als Pseudonyme (mit dichterischer Freiheit und phonetischer Rückung):
Améry $\widehat{=}$ Mayer Monroe $\widehat{=}$ Mortenson Garbo $\widehat{=}$ Gustafsson

[3] In der experimentellen Lyrik benutzt von *Otto Promber, Oskar Pastior, Herbert Pfeiffer*.

Reger Renner Rentner Reittier Marktkram Lagerregal Regiegeiger Reliefpfeiler
Eine Xenie Salomo las Nur Du, Gudrun Plaudere, du Alp Oh Cello voll Echo
Erika feuert nur untreue Fakire Ein Neger mit Gazette zagt im Regen nie
Eins nutzt uns: Amore. Die Rederei da, die Rederei der Omas, nutzt uns nie

Im Englischen sind bekannte Palindrome:

red rum and murder a man, a plan, a canal: panama ma is as selfless as i am
was it a cat i saw *(Dudeney)* madam, i'm adam *(Sam Loyd)*
doc note, i dissent. a fast never prevents a fatness. i diet on cod *(Peter Hilton)*

Martin Gardner verdanken wir:

Esope reste ici et se repose in girum imus nocte et consumimur igni

6.1.2 Schüttelreim: Eine harmlose nichtkryptographische Verwendung der Transposition findet man im Schüttelreim (engl. *spoonerism*):

schwarzen Wein – Warzenschwein
fiesen Rächer – Riesenfächer
Federn lassen – ledern fassen
reine Sache – seine Rache
they hung flags – they flung hags
dear old Queen – queer old Dean
wasted the term – tasted the worm
missed the history – hissed the mystery
Häuserlmeer – Mäuserlheer
tappen wir – Wappenti(e)r
Rotkehlchen – Kotröllchen
Gossensass – Sossengass

Die dabei benutzte Transposition π : $\pi(1,2,3,4) = (3,2,1,4)$ wird kryptographisch verwendet im **Medical Greek**, nach *Kahn* unter Londoner Medizinstudenten grassierend: POKE A SMIKE steht für *smoke a pipe*.

6.1.3 Würfel (engl. *route transcription*, '*tramp*'): Nach Wahl einer Zeilenlänge k als Kennzahl wird der Klartext waagrecht in Zeilen der Länge k geschrieben, senkrecht herausgelesen

```
i c h b i n
d e r d o k        I D T E C E O N H R R B B D E A I O I R N K S T
t o r e i s
e n b a r t
```

Dieses Verfahren haben wir schon zur Gewinnung eines Alphabets für einfache Substitutionen kennengelernt (3.2.5). Varianten lesen längs der Diagonalen,

Diagonalwürfel: E T N D O B I E R A C R E R H D I T B O S I K N

oder furchenwendig[4]: Jede zweite Gruppe wird im Krebs gelesen,

Schlangenlinienwürfel: I D T E N O E C H R R B A E D B I O I R T S K N

oder sogar die ganze Nachricht in einer Spirale,

Schneckenwürfel: T S K N I B H C I D T E N B A R I O D R E O R E .

Raffinierter sind **Rösselsprungwürfel** (Abb. 41); ihre unbefugte Entzifferung ist jedoch nicht schwierig, wenn der Anfang bekannt ist (Rösselsprung-Rätsel).

[4] bustrophedon, engl. *boustrophedonic*, in der Art der Ochsenkehre beim Pflügen.

1	4	53	18	55	6	43	20
52	17	2	5	38	19	56	7
3	64	15	54	31	42	21	44
16	51	28	39	34	37	8	57
63	14	35	32	41	30	45	22
50	27	40	29	36	33	58	9
13	62	25	48	11	60	23	46
26	49	12	61	24	47	10	59

Abb. 41. Rösselsprung-Würfel

An Stelle von Rechtecken wurden von Zeit zu Zeit andere geometrische Muster benutzt, hauptsächlich Dreiecke, aber auch Kreuze verschiedener Form und andere Anordnungen (Abb. 42, 43). Der Phantasie sind hier keine Grenzen gesetzt. Aber diese einfachen Transpositionsmethoden sind ganz offen für eine Kryptanalysis.

```
a       e       i       n       r       v       z
  b   d   f   h   k   m   o   q   s   u   w   v
    c       g       l       p       t       x
```

A E I N R V Z B D F H K M O Q S U W V C G L P T X

Abb. 42. *Rail Fence* (*Smith*); $n = 25$

```
  b     f     k     o     s     w
a   c e   g i   l n   p r   t v   x
  d     h     m     q     u     z
```

B F K O S W A C E G I L N P R T V X D H M Q U Z

Abb. 43. *Croix Grecque* (*Muller*), *Four winds* (*Nicols*); $n = 24$

6.1.4 Raster: Bequem handhabbar sind **Raster** (frz. *grille*, engl. *trellis cipher*). Man benötigt generell einen Satz von Rastern. Beim praktischen **Drehraster**[5] werden verschiedene Fenster ein-und desselben Rasters durch Drehung nacheinander zur Wirkung gebracht. Es gibt **2-zählige** (Abb. 44a) und **4-zählige** (Abb. 44b) Drehraster; in Unkenntnis des historischen Ursprungs werden sie auch Fleißner-Raster[6] genannt.

---

[5] Drehraster hat *Jules Verne* (1828–1905) in der Erzählung ‚Mathias Sandorff‘ (1885) beschrieben. Ihr Gebrauch ist schon im 18. Jahrhundert, beispielsweise 1745 in der Kanzlei des niederländischen Statthalters Wilhelm IV., nachgewiesen.
Der Mathematiker *C. F. Hindenburg* (1741–1808) hat sich 1796 mit Drehrastern beschäftigt, wie auch Moritz von Prasse 1799, Johann Ludwig Klüber 1809.

[6] *Eduard Fleißner von Wostrowitz*, österreich. Oberst, ‚Neue Patronen-Geheimschrift‘ (Handbuch der Kryptographie, Wien 1881). Das Wort ‚Patrone‘, von mittellat. *patronus*, ‚Vaterform‘, ‚Musterform‘, wurde in der Textiltechnik für eine Bindungsmuster-Zeichnung *auf kariertem Papier* verwendet.
In *Jaroslav Hašeks* Erzählung ‚Der tapfere Soldat Schwejk‘ wird ein ‚Handbuch der militärischen Kryptographie‘ von Oberleutnant *Fleißner* erwähnt, sowie andere Details, die eine gewisse Vertrautheit von *Hašek* mit der Kryptographie erkennen lassen.

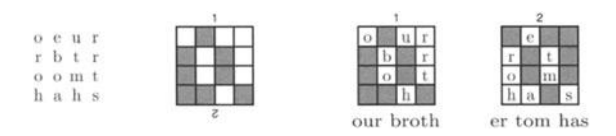


Abb. 44a. Zweizähliges Drehraster

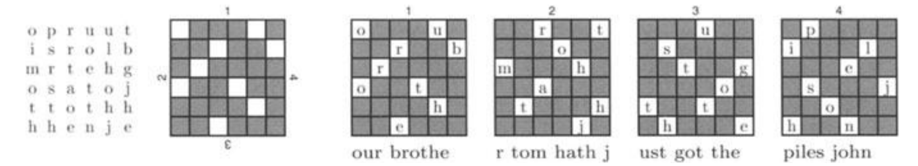


Abb. 44b. Vierzähliges Drehraster

Die Konstruktion von Drehrastern ist einfach: Man beschreibt einen Quadranten des Feldes (mit gerader Zeilen- und Spaltenanzahl) mit Markierungen, überlagert alle durch Rotation sich ergebenden Markierungen und wählt dann von jeder Markierung genau eine aus. Das Drehraster von Abb. 45 ergibt sich folgendermaßen:

1	2	3	7	**4**	1
4	5	**6**	8	5	**2**
7	**8**	9	9	6	3
3	6	9	**9**	8	7
2	5	8	6	**5**	4
1	4	**7**	3	2	1

Damit lassen sich Raster auch nach Schlüsseln herstellen, die die Rasterlagen in den sukzessiven Schritten festlegen, etwa[7] suggestiv wie folgt:



Würfel und Drehraster wurden gern auf militärisch-taktischem Niveau verwendet. Im 1. Weltkrieg wurden vom deutschen Heer ab Anfang 1917 Drehraster verwendet, mit Bezeichnungen wie *ANNA* (5×5), *BERTA* (6×6), *CLARA* (7×7), *DORA* (8×8), *EMIL* (9×9) und *FRANZ* (10×10). Nach vier Monaten gab man das wieder auf.

Würfel und Drehraster ergeben eine Transposition der gesamten Nachricht. Vorläufer ist das Raster von *Cardano*, das *keine* Transposition ergibt, sondern nur neben die durch die Fenster sichtbaren Zeichen eine größere Menge von Blendern setzt (vgl. 1.6). Ernstzunehmen sind diese Verfahren für sich allein nicht, aber man ist nie sicher, ob sie nicht doch verwendet werden: In Verbindung mit Substitution ist Transposition jedenfalls sehr wirksam.

---

[7] Für $n = 4\nu^2$ Felder ergeben sich
zweizählig: $2^{n/2}$ Möglichkeiten, vierzählig: $4^{n/4} = 2^{n/2}$ Möglichkeiten. Für $n = 36$ sind das $\approx 2.62 \cdot 10^5$, die Anzahl aller Permutationen beträgt $36! \approx 3.72 \cdot 10^{41}$.

6.2 Spalten-Transpositionen

6.2.1 Mit Kennwörtern arbeitet die Verfahrensklasse der **einfachen Spaltentransposition** (engl. *columnar transposition*, frz. *tranposition simple à clef*). Die Nachricht wird in Zeilen der gewählten Länge k geschrieben, die entstehenden Spalten werden nach Maßgabe einer Permutation $\pi \in \gamma_k$ (‚Losung') umgeordnet und senkrecht herausgelesen:

$\underbrace{\text{e s w a r s c h o n d u n k e l}}$ $\pi:$ *2 1 4 3*

2 1 4 3	*1 2 3 4*	
e s w a	S E A W	
r s c h	S R H C	S S N K E R O N A H U L W C D E .
o n d u	N O U D	
n k e l	K N L E	

Für die Kryptanalyse damit äquivalent ist, die nach Maßgabe von $\pi \in \gamma_k$ umgeordneten Spalten waagrecht herauszulesen.

$\underbrace{\text{e s w a r s c h o n d u n k e l}}$ $\pi:$ *2 1 4 3*

2 1 4 3	*1 2 3 4*	
e s w a	S E A W	
r s c h	S R H C	S E A W S R H C N O U D K N L E .
o n d u	N O U D	
n k e l	K N L E	

Dies kann auch als eine **Blocktransposition** (‚Umstellung' oder ‚Gruppen-Transposition', *Gaines: complete-unit transposition, Eyraud: Variante de Richelieu*) aufgefaßt werden: Die Nachricht wird in Blöcke von k Elementen unterteilt und jeder dieser Blöcke wird mittels $\pi \in \gamma_k$ permutiert – es handelt sich um eine monoalphabetische polygraphische Chiffrierung mit der Breite k.

Die einfache Spaltentransposition ist aber mit Papier und Bleistift mit weniger Mühe und sicherer durchzuführen. Und obwohl einfache Spaltentransposition über die ganze Nachricht permutiert, bietet sie nicht mehr Sicherheit als Blocktransposition – hier liegt auch eine *complication illusoire* vor.

6.2.2 Um die Dechiffrierung zu erleichtern, wird beim Würfel wie auch bei einfacher Spaltentransposition und Blocktransposition meist verlangt, daß die Länge der Nachricht durch k teilbar ist. Die dazu erforderlichen Blender sind, wenn sie nicht fachmännisch gewählt werden – wenn also z.B. mit qq … q aufgefüllt wird – ein beliebter Ansatz für den unbefugten Entzifferer. Notwendig ist diese Aufweichung beim Würfel wie bei der Spaltentransposition nicht – man kann ja die Länge der letzten Zeile, der Restzeile als Divisionsrest erhalten.

Einfache Spaltentransposition und Blocktransposition – auch mit unvollständig ausgefüllten Rechtecken – sind mit simpelsten Mitteln zu lösen. Man geht deshalb gern zu komplizierteren Transpositionen über. Sie sind alle als zusammengesetzte Verfahren (siehe 9.1.1) auffaßbar.

6.2.3 Mit einer *zusätzlichen* Permutation π_1 arbeitet die **gemischte Zeilen-Spalten-Transposition**, frz. *transposition double* (*Givierge, Eyraud*).[8] Bei ihr wird zuerst die Nachricht zeilenweise nach Maßgabe einer Permutation π_1 *hineingeschrieben*, dann werden die Spalten wie vorhin umgeordnet nach Maßgabe einer Permutation $\pi_2 \in \gamma_k$, sodann wird *spaltenweise* die Geheimnachricht *herausgelesen*:

e s w a r s c h o n d u n k e l π_1 : *2 4 1 3* π_2 : *2 1 4 3*

			2 1 4 3	*1 2 3 4*	
1	e s w a	*2*	r s c h	S R H C	
2	r s c h	*4*	n k e l	K N L E	S K S N R N E O H L A U C E W D .
3	o n d u	*1*	e s w a	S E A W	
4	n k e l	*3*	o n d u	N O U D	

Ebenso wird bei der **gemischten Zeilen-Block-Transposition** vorgegangen, jedoch wird die Geheimnachricht *zeilenweise* herausgelesen:

e s w a r s c h o n d u n k e l π_1 : *2 4 1 3* π_2 : *2 1 4 3*

			2 1 4 3	*1 2 3 4*	
1	e s w a	*2*	r s c h	S R H C	
2	r s c h	*4*	n k e l	K N L E	S R H C K N L E S E A W N O U D .
3	o n d u	*1*	e s w a	S E A W	
4	n k e l	*3*	o n d u	N O U D	

Der selbe Effekt kann erreicht werden, wenn π_1 hinterher durchgeführt wird:

e s w a r s c h o n d u n k e l π_2 : *2 1 4 3* π_1 : *2 4 1 3*

2 1 4 3	*1 2 3 4*				
e s w a	S E A W	*1*	S R H C	*2*	
r s c h	S R H C	*2*	K N L E	*4*	S R H C K N L E S E A W N O U D .
o n d u	N O U D	*3*	S E A W	*1*	
n k e l	K N L E	*4*	N O U D	*3*	

Bei der gemischten Zeilen-Spalten-Transposition oder Zeilen-Block-Transposition mit *quadratischer* Anordnung kann man beide Male die gleiche Losung verwenden: $\pi_1 = \pi_2$. Setzt man aber $\pi_1 = \pi_2^{-1}$, so handelt es sich um die Methode, die *Auguste Kerckhoffs* 1883 den russischen Nihilisten zuschrieb (*nihilist cipher*).

Zur mathematischen Behandlung dieser Transpositionen soll die Nachricht x stets durch eine Matrix X von l Zeilen der Länge k dargestellt sein.

Zeilenpermutation bedeutet Multiplikation
von links mit einer $l \times l$-Permutationsmatrix $\pi_1 \ : X \mapsto \pi_1 X$,
Spaltenpermutation bedeutet Multiplikation
von rechts mit einer $k \times k$-Permutationsmatrix $\pi_2 \ : X \mapsto X \pi_2$.

[8] Beachte den Unterschied im Französischen: *double transposition* (6.2.4), *transposition double* (6.2.3).

Letzteres ist gerade die Block-Transposition. Die Spalten-Transposition jedoch ergibt sich als eine Spaltenpermutation, gefolgt von einer Matrix-Transposition $.^T$ (d.h. einem Würfel)

$$X \mapsto (X\pi_2)^T ,$$

somit auch als Zeilenpermutation mit[9] π_2^{-1}, angewandt auf die transponierte Matrix X^T:

$$X \mapsto \pi_2^{-1} X^T .$$

Eine gemischte Zeilen-Block-Transposition stellt sich dar als

$$X \mapsto (\pi_1 X)\pi_2 = \pi_1(X\pi_2) .$$

Eine gemischte Zeilen-Spalten-Transposition stellt sich dar als

$$X \mapsto ((\pi_1 X)\pi_2)^T = \pi_2^{-1} X^T \pi_1^{-1} .$$

Im Fall $\pi_1 = \pi^{-1}$, $\pi_2 = \pi$ der Nihilisten-Methode wird die gemischte Zeilen-Block-Transformation zur Ähnlichkeitstransformation

$$X \mapsto \pi^{-1} X \pi ,$$

die gemischte Zeilen-Spalten-Transposition ergibt hingegen

$$X \mapsto \pi^{-1} X^T \pi .$$

6.2.4 Die **doppelte Spalten-Transposition** (‚Doppelwürfel', engl. *double columnar transposition*, frz. *double transposition*) wendet zweimal Spaltentransposition an. An sich müßte dabei jedesmal eine andere Losung verwendet werden; dies geschieht bei quadratischer Anordnung nicht immer.

Eine doppelte Spalten-Transposition *mit quadratischer Anordnung* ergibt

$$X \mapsto ((X\pi)^T \pi')^T = (\pi')^{-1} X \pi ,$$

ist also von einer gemischten Zeilen-Block-Transposition nicht zu unterscheiden[10]; beide Verfahren können im Prinzip bereits mit den Methoden, die für einfache Spaltentransposition geeignet sind, gebrochen werden.

Die quadratische Anordnung lag auch vor bei der Version der amerikanischen Armee (‘*U.S. Army Double Transposition*’), die doppelte Spaltentransposition mit einer einzigen Losung[11] verwendete. Gleichermaßen verfuhr man beim kaiserlichen Heer, das das Verfahren arglos verwendete — die Franzosen unter dem damaligen Capitaine *François Cartier* nannten es *übchi* und lasen bis zum 18. November 1914 mit.

Erstaunlicherweise hatte die deutsche Wehrmacht nichts daraus gelernt und kehrte zu ihren Sünden zurück: Von Kriegsausbruch bis 1. 7. 1941 und wieder ab 1. 6. 1942 diente die doppelte Spaltentransposition mit täglich wechselnder Losung beim Heer als „Handschlüsselverfahren“, das vom Regiment abwärts

---

[9] Da eine Permutationsmatrix orthogonal ist, ist $\pi_1^T = \pi_1^{-1}$.

[10] Beide werden wesentlich durch ein Kreuzprodukt $\pi_i \times \pi_k$ dargestellt.

[11] Es handelt sich also ebenfalls um eine Ähnlichkeitstransformation.

verwendet wurde, und bei der Marine als „Reserve-Handverfahren“ (Notschlüssel). Diesmal lasen die Briten mit. Die Verwendung zweier verschiedener Losungen hatte den Einbruch nicht verhindert, auch dreifache Spaltentransposition hätte da nichts genützt: Die einschlägige Methode, das „multiple Anagrammieren“ (21. Kapitel), war davon völlig unabhängig.

Doppelte Spaltentransposition wurde im 2. Weltkrieg auch von den Agenten der britischen Spionage- und Sabotageorganisation *Special Operations Executive* (S.O.E.) verwendet. Darüber hat neuerdings *Leo Marks* berichtet.

6.2.5 Eine echte Komplikation für die unbefugte Entzifferung von einfachen Transpositionen ist die Einführung von unregelmäßig verstreuten Plätzen, die nicht beschrieben werden dürfen: PA-K2-System, Japan 1941; Heftschlüsselverfahren der deutschen Wehrmacht (1937), das ein 13×13-Raster mit 10 freien Plätzen pro Zeile und Spalte benützt; sowie der sogleich zu besprechende Rasterschlüssel 44 der Deutschen Wehrmacht, ab März 1944.

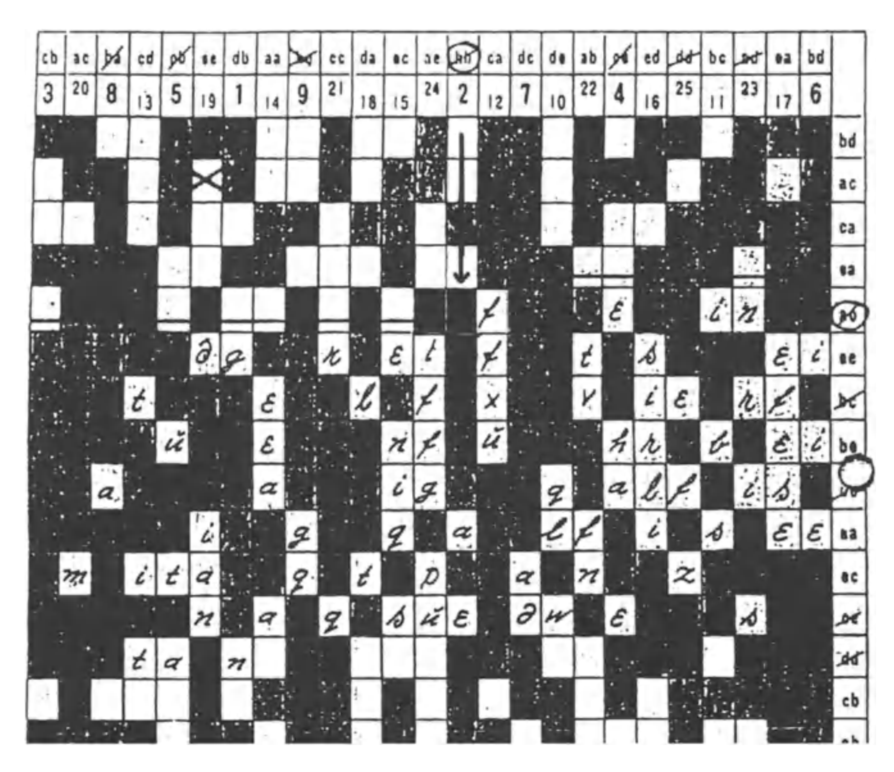


Abb. 45. Rasterschlüssel 44 der Deutschen Wehrmacht (März 1944)

Die USA brachen die PA-K2–Chiffrierung regelmäßig, wenn auch oft mit ziemlicher Verzögerung. Dem Rasterschlüssel 44 ging es nicht viel besser, da die Briten nach der Landung in der Normandie eine Menge Unterlagen erbeuteten. Immerhin hatten nicht nur die Briten in Bletchley Park ihre Probleme, auch die Deutschen mußten das komplizierte Verfahren erst erlernen.

Abb. 45 gibt ein Beispiel aus der Schlüsselanleitung, Ausgabe 27. März 1944 für das von den Briten *crossword puzzle* genannte Verfahren: Der Klartext

Feind greift seit 11.45 Uhr bei Orchejow mit 8 Panzern nach Südwesten an

wurde zunächst vorschriftsgemäß aufbereitet, wobei *ch* durch q ersetzt wurde und der Ortsname, in aa und ee eingeschlossen, verdoppelt und überchiffriert wurde mit einem ‚Ortsnamenalphabet', hier

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
n	m	l	y	a	x	w	f	u	q	t	d	z	r	i	v	k	g	e	o	p	j	s	h	b	c

Orjechow ergibt so igqalfis, insgesamt entsteht der Text

feindgreiftseitelfxvierfuenfuhrbeiaaigqalfisigqalfiseemitaqtpanznaqsuedwestan

der aus 77 Zeichen besteht (Grenzen: mindestens 60, höchstens 200 Zeichen).

Die Eintragung der Nachricht auf die freien Plätze (10 pro Zeile bei maximal 24 Zeilen) der täglich wechselnden Rasterschablone erfolgt zeilenweise; das Anfangsfeld wird willkürlich gewählt — etwa Spalte `bb` und Zeile `ae`.

Diese Schlüsselvereinbarung wird der Nachricht in einem Spruchkopf vorausgeschickt, der neben dem Klarspruchschlüssel `bbae`, nach einer auf der Rückseite der Schablone befindlichen Tabelle homophon chiffriert, auch die taktische Zeit und die gesamte Zeichenanzahl des Spruchs enthält, also etwa `1203-77-tuzd` lautet.

Aus der Minutenzahl und der Zeichenanzahl wird die Quersumme gebildet — hier 0+3+7+7= 17 — und von der Anfangsspalte `bb` um eben so viele Spalten — hier 17 — weitergezählt. Dies ergibt hier `ee`, und mit dieser Spalte beginnt das der vorgegebenen Spaltennumerierung folgende Herauslesen des zu übermittelnden Chiffrats, das da lautet

```
1203-77-tuzd
dianm rqtvf nnris iffgp uefzg naeeh aeuta iiead
agqql wibsf fxuti teeaa eniqs sirli efese lt      .
```

Man überzeugt sich leicht, daß die Dechiffrierung durch Umkehrung der Reihenfolge der geschilderten Schritte eindeutig bestimmt ist.

6.2.6 Viele Möglichkeiten gibt es für die Gewinnung der bei der Transposition benutzten Permutationen aus Kennwörtern, vor allem aus Merkworten oder -versen. Eine in der Literatur häufig erwähnte geht wie folgt vor:

Man ordnet jedem Buchstaben des Kennworts die Platznummer zu, die es in der alphabetischen Rangfolge hat:

M	*A*	*C*	*B*	*E*	*T*	*H*
6	*1*	*3*	*2*	*4*	*7*	*5*

Das geht jedoch nur, wenn das Kennwort keine wiederholten Buchstaben hat. Andernfalls wird das Verfahren geringfügig modifiziert: Wiederholt auftretende Buchstaben werden konsekutiv numeriert:

A	*M*	*B*	*A*	*S*	*S*	*A*	*D*	*E*	*D*	*A*	*L*	*L*	*E*	*M*	*A*	*G*	*N*	*E*
1	*15*	*6*	*2*	*18*	*19*	*3*	*7*	*9*	*8*	*4*	*13*	*14*	*10*	*16*	*5*	*12*	*17*	*11*

6.3 Anagramme

Transposition läßt den Zeichenhaufen[12] einer Nachricht unverändert. Beim **Anagramm** sucht man aus dem Zeichenhaufen die Nachricht zu rekonstruieren. Eine systematisches Lösungsverfahren würde alle Transpositionsverfahren wertlos machen.

6.3.1 *Huyghens* gab folgendes Anagramm

$a^7\ c^5\ d^1\ e^5\ g^1\ h^1\ i^7\ l^4\ m^2\ n^9\ \ o^4\ p^2\ q^1\ r^2\ s^1\ t^5\ u^5$,

woraus man '*annulo cingitur tenui plano, nusquam cohaerente, ad eclipticam inclinato*' („[Saturn] ist umgeben von einem dünnen flachen Ring, der ihn nirgendwo berührt und zur Ekliptik geneigt ist") erhalten kann.

Newton schrieb an Leibniz

$a^7\ c^2\ d^2\ e^{14}\ f^2\ i^7\ l^3\ m^1\ n^8\ \ o^4\ q^3\ r^2\ s^4\ t^8\ v^{12}\ x^1$,

was als '*data aequatione quodcumque fluentes quantitates involvente, fluxiones invenire et vice versa*' („aus einer beliebig viele Fluenten enthaltenden Gleichung die Fluxionen zu finden und umgekehrt") gedeutet wird.

Anagramme waren unter Wissenschaftlern des 17. Jahrhunderts sehr beliebt, was vielleicht mit der Vorliebe, die Amateure bis heute für Transposition hegen, zusammenhängt. *Galilei* schrieb an *Kepler* ein maskiertes Anagramm:

HAEC IMMATURA A ME IAM FRUSTRA LEGUNTUR O. Y.

(„Diese unreifen Dinge lese ich vergeblich"), was bedeuten soll '*cynthiae figuras aemulatur mater amorum*' („Die Mutter der Liebe [= Venus] ahmt die Phasen der Cynthia [= Mond] nach").

Wissenschaftler achteten damals sehr auf Priorität: Noch *Carl Friedrich Gauß* publizierte am 25. April 1812 ein ihm wichtig genug erscheinendes Ergebnis über die Störungen der Jupiterbahn durch den kleinen Planeten Pallas durch die vermutlich binär zu verstehende Chiffre IIIIOOOIOOIOIOOI.

Ludwig II. von Bayern schrieb das (nicht tiefliegende) maskierte Anagramm MEICOST ETTAL, was als *l'état c'est moi* zu lesen ist.

Ein modernes Beispiel ist ASTRONOMERS, was als *moon starters* , aber auch als *no more stars* gelesen werden kann.

Auch die pharmazeutische Industrie kennt Anagramme: Hinter dem Warenzeichen KLINOMYCIN® (Lederle) verbirgt sich der Wirkstoff *Minocyclin.*

In der experimentellen Lyrik findet man Anagramm-Gedichte wie[13]

Glück und Sommer weinen Wade, Röhricht neu,
Rad und Röcke suchen Note: Glühweinwimmern.
Randenhügel, Wut und Nock: wie Öre schimmern.
Wandertürme, Gnom in Köchern wund, eil scheu.

vom Typ $a^1\ c^2\ d^2\ e^5\ g^1\ h^2\ i^2\ k^1\ l^1\ m^2\ n^4\ o^1\ r^3\ s^1\ t^1\ u^2\ w^2\ ö^1\ ü^1$.

---

[12] d.h. Wiederholungen mitgerechnet. Die Aussage ist auch richtig für Zeichenmengen.
[13] *Francesco Gagliardi.*

Unter britischen Intellektuellen sind Anagramme auch heute noch beliebt (Abb. 46). Sie finden sich weiterhin in Berufsrätseln:

IRI BRÄTER, GENF	Briefträgerin
FRANK PEKL, REGEN	Krankenpfleger
PEER ASTIL, MELK	Kapellmeister
INGO DILMUR, PEINE	Diplomingenieur
EMIL REST, GERA	Lagermeister
KARL SORDORT, PEINE	Personaldirektor
GUDRUN SCHRILL, HERNE	Grundschullehrerin

6.3.2 Die Frage drängt sich auf, ob man nicht aus einem Haufen von Buchstaben auch mehrere Nachrichten gewinnen kann. Schon *Jonathan Swift* beschäftigte sich damit, als er in seiner Satire ‚Gullivers Reisen' darauf hinwies, ein böser politischer Gegner könnte aus einem so harmlosen Satz wie OUR BROTHER TOM HATH JUST GOT THE PILES durch die *'Anagrammatick Method'* herauslesen *Resist, — a Plot is brought home — The Tour.*

In der Tat zeigt die Erfahrung, bestätigt durch *Shannon*s Theorie, daß es für ein Anagramm keine Unizitätslänge gibt.

admonition	domination	alarmingly	marginally
algorithms	logarithms	alienators	senatorial
ancestries	resistance	antagonist	stagnation
auctioning	cautioning	australian	saturnalia
broadsides	sideboards	catalogued	coagulated
catalogues	coagulates	certifying	rectifying
collapsing	scalloping	compressed	decompress
configures	refocusing	conserving	conversing
contenting	contingent	coordinate	decoration
countering	recounting	creativity	reactivity
dealership	leadership	decimating	medicating
decimation	medication	deductions	discounted
denominate	emendation	denotation	detonation
denouncers	uncensored	deposition	positioned
descriptor	predictors	directions	discretion
discoverer	rediscover	earthiness	heartiness
egocentric	geocentric	enduringly	underlying
enervating	venerating	enervation	veneration
excitation	intoxicate	filtration	flirtation
harmonicas	maraschino	impregnate	permeating
impression	permission	impressive	permissive
indescreet	iridescent	introduces	reductions
mouldering	remoulding	nectarines	transience
ownerships	shipowners	percussion	supersonic
persistent	prettiness	persisting	springiest
pertaining	repainting	petitioner	repetition
platitudes	stipulated	positional	spoliation
procedures	reproduces	profounder	underproof

Abb. 46. Zehn-Buchstaben-Wort-Anagramme (nach *Hugh Casement*)

Zur Historie wäre noch anzumerken, daß sich eine erste Frühform der Transposition im griechischen *Skytale* ($\sigma\kappa\upsilon\tau\alpha\lambda\varepsilon$), bereits aus dem 5. Jahrhundert v. Chr. bekannt, findet: Ein Stab, um den ein Pergamentstreifen gewickelt wird, auf den die Nachricht — der Länge des Stabes nach — geschrieben

wird. Nach dem Niedergang der klassischen Kultur findet sich die erste Chiffrierung durch Transposition in mittelalterlichen Mönchshandschriften, wie *Bernhard Bischoff* erforscht hat: Krebs und senkrechte Schrift, gelegentlich in Verbindung mit Wortspielen.

Transposition erfreute sich in unserem Zeitalter keiner großen Beliebtheit mehr. Der Grund liegt in Schwierigkeiten der Mechanisierung: Man braucht große Speicher, um effektiv mit Transposition verschlüsseln zu können. Mit der Verfügbarkeit von Halbleiterspeichern für Millionen von Bits, mit kurzer Zugriffszeit, kann sich das jedoch bald ändern. Das 21. Jahrhundert wird eine Rückkehr der Transposition zu ihrer wahren Wichtigkeit sehen.

7 Polyalphabetische Chiffrierung: Begleitende und unabhängige Alphabete

Monoalphabetische Chiffrierung benutzt irgend einen (womöglich polygraphischen) Chiffrierschritt ständig. Alle im 3. bis 6. Kapitel behandelten Chiffrierschritte können monoalphabetisch verwendet werden – das wurde in den Beispielen auch stillschweigend angenommen.

Eine echte polyalphabetische Chiffrierung erfordert, daß das Chiffrierschritt-System M mindestens die Kardinalität $\theta = 2$ hat, d.h. daß die Menge M der verfügbaren Chiffrierschritte mindestens zweielementig ist. Für den häufigen Fall $\theta = N$ spricht man von einer *chiffre carré*.

Die einzelnen Chiffrierschritte können verschiedenster Natur sein; so könnte das Chiffriersystem M beispielsweise eine Anzahl einfacher Substitutionen und eine Anzahl Transpositionen der Breite 4 umfassen. In der Regel verlangt man aber, daß alle Chiffrierschritte ein und der selben Klasse angehören – beispielsweise der Klasse der Substitutionen, oder der linearen Substitutionen, oder der Transpositionen. Oft wird auch verlangt, daß alle Chiffrierschritte gleiche Chiffrierbreite besitzen, was zur Blockchiffrierung führt.

Das Hauptproblem ist, auf einfache Weise viele verschiedene Chiffrierschritte festzulegen oder, wie man sagt, viele verschiedene Alphabete zu erzeugen. Erstaunlicherweise hat die Phantasie der Erfinder dabei noch vieles offen gelassen.

7.1 Potenzierung

Es liegt nahe, das Chiffriersystem dadurch aufzubauen, daß man aus einem Grundschritt andere Chiffrierschritte ableitet. Insbesondere für eine einfache Substitution haben wir in 3.2.4 bereits Familien von **begleitenden** Alphabeten angetroffen, nämlich durch ‚Verschiebung' und durch ‚Potenzierung' entstehende. Wir beschränken uns auf den endomorphen Fall $V \doteq W$, $m = n$.

Wir werden sehen, daß diese beiden Familien mittels des Begriffs der iterierten Substitution S^i entstehen, definiert durch $p\,S^{j+1} = p\,S\,S^j$ für eine endomorphe Substitution S. In der Tat, iterierte Substitution ist vorherrschend bei der Erzeugung begleitender Alphabete.

7.1.1 Sei allgemein $S : Q^n \leftarrow\!\!\!\rightarrow Q^n$. Zur Gewinnung von Familien begleitender Chiffrierschritte kennen wir also bereits

$\{ S^i : i \in \mathbb{N} \}$, die Gruppe der **potenzierten S-Alphabete**.

Mit festen Substitutionen $P_1 : V \leftarrow\!\!\!\rightarrow Q^n$ und $P_2 : Q^n \leftarrow\!\!\!\rightarrow W$ bieten sich an die Mengen von Chiffrierschritten

a) $\{ P_1 S^i P_2 : i \in \mathbb{N} \}$, wo $P_1 S^i P_2 : V \leftarrow\!\!\!\rightarrow W$.

Ferner haben wir mit einer weiteren festen Substitution $R : Q^n \leftarrow\!\!\!\rightarrow Q^n$

$\{ S^{-i} R S^i : i \in \mathbb{N} \}$, die Gruppe der **$S$-Ähnlichkeiten** von R.

Wieder bieten sich mit Substitutionen $P_1 : V \leftarrow\!\!\!\rightarrow Q^n$ und $P_2 : Q^n \leftarrow\!\!\!\rightarrow W$ an die Mengen von Chiffrierschritten

b) $\{ P_1 S^{-i} R S^i P_2 : i \in \mathbb{N} \}$, wo $P_1 S^{-i} R S^i P_2 : V \leftarrow\!\!\!\rightarrow W$.

Die Mengen sind jedenfalls endlich, denn $Q^n \leftarrow\!\!\!\rightarrow Q^n$ mit endlichem $|Q| = N$ umfaßt nur $(N^n)!$ verschiedene Permutationen.

Ist S von der Ordnung $h \le (N^n)!$, d.h. ist $S^h = I$ und $S^i \ne I$ für $i < h$, so liefert die Potenzierung h verschiedene Alphabete. Beachte, daß $h > N^n$ möglich ist: Für $N = 5$, $n = 1$ ist die Substitution (in Zyklenschreibweise) $(ab)(cde)$ von der Ordnung 6. h kann aber auch recht klein sein: Ist S involutorisch, so liefert die Potenzierung außer I keinen begleitenden Chiffrierschritt.

7.1.2 Vorteilhaft mag es sein, für S eine voll zyklische Permutation σ zu wählen. Eine solche Permutation ist von der Ordnung N^n . Es gibt $(N^n - 1)!$ verschiedene voll zyklische Permutationen. Die reine Potenzierung kann in diesem Fall, wie schon in 3.2.8 (Abb. 28) erwähnt, durch eine einzige Scheibe (oder ein einziges Lineal) mit dem Zyklus σ und zwei Fenster – ein Klartextfenster und ein Geheimtextfenster – mechanisiert werden. Man wird dabei, wenn N von der Größenordnung 25 ist, über $n = 2$ kaum hinausgehen.

7.2 Verschobene und rotierte Alphabete

Hat man in Q ein Standardalphabet ausgezeichnet, so ist auch in Q^n durch die lexikographische Ordnung ein Standardalphabet bestimmt. Mit ρ soll speziell der dazu gehörige Zyklus (3.2.3) des Standardalphabets bezeichnet werden. Es ist also in 7.1.1 $S = \rho$ und $S^i = \rho^i$.

7.2.1 $\{ \rho^i : i \in \mathbb{N} \} = \{ \rho^i \rho : i \in \mathbb{N} \} = \{ \rho \rho^i : i \in \mathbb{N} \}$ wird speziell als Menge der **verschobenen Standardalphabete**, frz. *alphabets normalement parallèles* bezeichnet.

Allgemeiner, wenn nur eine Substitution/Permutation P („P-Alphabet", **Referenzalphabet**, engl. *primary (mixed) alphabet*) frei gewählt wird:

a′) $\{ \rho^i P : i \in \mathbb{N} \}$ und a″) $\{ P \rho^i : i \in \mathbb{N} \}$ wird als

Menge der (horizontal bzw. vertikal) **verschobenen P-Alphabete**, frz. *alphabets désordonnés parallèles* bezeichnet. Für den allgemeinen Fall $\{ P_1 \rho^i P_2 : i \in \mathbb{N} \}$ von 7.1.1 a) siehe 8.2.3 (und 19.5.3).

Die Bezeichnungen werden klar, wenn man einen Blick wirft auf die nachfolgenden Tafeln für die Familien von Substitutionen: Mit $V = Q = W = Z_{26}$ und $N = 26$, für das durch das Kennwort NEWYORKCITY erzeugte Referenzalphabet P,

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
N	E	W	Y	O	R	K	C	I	T	A	B	D	F	G	H	J	L	M	P	Q	S	U	V	X	Z

ergibt die Menge $\{\ \rho^i P : i \in \mathbb{N}\}$ die folgende Tafel (in der Form einer *tabula recta*, d.h., mit identischen Buchstaben längs der Gegendiagonalen)

i	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	N	E	W	Y	O	R	K	C	I	T	A	B	D	F	G	H	J	L	M	P	Q	S	U	V	X	Z
1	E	W	Y	O	R	K	C	I	T	A	B	D	F	G	H	J	L	M	P	Q	S	U	V	X	Z	N
2	W	Y	O	R	K	C	I	T	A	B	D	F	G	H	J	L	M	P	Q	S	U	V	X	Z	N	E
3	Y	O	R	K	C	I	T	A	B	D	F	G	H	J	L	M	P	Q	S	U	V	X	Z	N	E	W
4	O	R	K	C	I	T	A	B	D	F	G	H	J	L	M	P	Q	S	U	V	X	Z	N	E	W	Y
5	R	K	C	I	T	A	B	D	F	G	H	J	L	M	P	Q	S	U	V	X	Z	N	E	W	Y	O
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
25	Z	N	E	W	Y	O	R	K	C	I	T	A	B	D	F	G	H	J	L	M	P	Q	S	U	V	X

während die Menge $\{\ P\rho^i : i \in \mathbb{N}\}$ die folgende Tafel hat

i	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	N	E	W	Y	O	R	K	C	I	T	A	B	D	F	G	H	J	L	M	P	Q	S	U	V	X	Z
1	O	F	X	Z	P	S	L	D	J	U	B	C	E	G	H	I	K	M	N	Q	R	T	U	W	Y	A
2	P	G	Y	A	Q	T	M	E	K	V	C	D	F	H	I	J	L	N	O	R	S	U	V	X	Z	B
3	Q	H	Z	B	R	U	N	F	L	W	D	E	G	I	J	K	M	O	P	S	T	V	W	Y	A	C
4	R	I	A	C	S	V	O	G	M	X	E	F	H	J	K	L	N	P	Q	T	U	W	X	Z	B	D
5	S	J	B	D	T	W	P	H	N	Y	F	G	I	K	L	M	O	Q	R	U	V	X	Y	A	C	E
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
24	L	C	U	W	M	P	I	A	G	R	Y	Z	B	D	E	F	H	J	K	N	O	Q	S	T	V	X
25	M	D	V	X	N	Q	J	B	H	S	Z	A	C	E	F	G	I	K	L	O	P	R	T	U	W	Y

Bei den *horizontal* verschobenen P-Alphabeten tritt das P-Alphabet in jeder Zeile in Erscheinung, von Zeile zu Zeile um eine Stelle nach links verschoben; bei den *vertikal* verschobenen P-Alphabeten ist das Referenzalphabet P nur in der ersten Zeile erkennbar, dafür tritt das Standard-Alphabet vertikal auf.

7.2.2 $\{\ \rho^{-i} R \rho^i : i \in \mathbb{N}\ \}$ ist die
Menge der R-**rotierten** (zu R ‚ähnlichen') **Standardalphabete**
(die Bezeichnung wird in 7.3 motiviert werden)

Etwas allgemeiner, für den besonderen Fall $P_1 = P$, $P_2 = P^{-1}$ von 7.1.1 b):

b*) $\{\ P\rho^{-i} R \rho^i P^{-1} : i \in \mathbb{N}\ \}$ ist die
Menge der R-**rotierten** P-**Alphabete**.

Nimmt man für R das zum selben Kennwort NEWYORKCITY gehörige Referenzalphabet wie oben, so ergibt die Menge $\{ \rho^{-i} R \rho^i : i \in \mathbb{N} \}$ die Tafel

i	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	N	E	W	Y	O	R	K	C	I	T	A	B	D	F	G	H	J	L	M	P	Q	S	U	V	X	Z
1	A	O	F	X	Z	P	S	L	D	J	U	B	C	E	G	H	I	K	M	N	Q	R	T	V	W	Y
2	Z	B	P	G	Y	A	Q	T	M	E	K	V	C	D	F	H	I	J	L	N	O	R	S	U	W	X
3	Y	A	C	Q	H	Z	B	R	U	N	F	L	W	D	E	G	I	J	K	M	O	P	S	T	V	X
4	Y	Z	B	D	R	I	A	C	S	V	O	G	M	X	E	F	H	J	K	L	N	P	Q	T	U	W
5	X	Z	A	C	E	S	J	B	D	T	W	P	H	N	Y	F	G	I	K	L	M	O	Q	R	U	V
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
21	M	F	X	D	O	V	W	Y	A	B	C	E	G	H	K	L	N	P	Q	S	U	I	Z	R	T	J
22	K	N	G	Y	E	P	W	X	Z	B	C	D	F	H	I	L	M	O	Q	R	T	V	J	A	S	U
23	V	L	O	H	Z	F	Q	X	Y	A	C	D	E	G	I	J	M	N	P	R	S	U	W	K	B	T
24	U	W	M	P	I	A	G	R	Y	Z	B	D	E	F	H	J	K	N	O	Q	S	T	V	X	L	C
25	D	V	X	N	Q	J	B	H	S	Z	A	C	E	F	G	I	K	L	O	P	R	T	U	W	Y	M

Bei den *R-rotierten* P-Alphabeten tritt das Referenzalphabet R nur in der ersten Zeile auf, und wird *längs der Diagonalen* in der Reihenfolge von P fortgesetzt (‚diagonal verschobene Standard- bzw. P-Alphabete‘).

7.2.3 Die Familie der horizontal verschobenen P-Alphabete kann mechanisiert werden, wie in 3.2.7 (Abb. 26) gezeigt, durch eine *Alberti*-Scheibe, die (außen) das Standardalphabet und drehbar (innen) das permutierte Alphabet P trägt oder durch einen Schieber, wobei eines der Alphabete wiederholt werden muß.. Wir werden deshalb kurz von ALBERTI-**Chiffrierschritten** im Falle der horizontal verschobenen P-Alphabete, und entsprechend von ROTOR-**Chiffrierschritten** im Falle der R-rotierten Standardalphabete oder P-Alphabete sprechen.

7.2.4 Die Zyklenzerlegung der begleitenden Alphabete ist interessant.

Beispiel: Für $Q = \begin{pmatrix} \text{a b c d e} \\ \text{B A D E C} \end{pmatrix} = (\text{a b})\,(\text{c d e})$ und $\rho = (\text{a b c d e})$,

ergibt sich

$$\rho Q = \begin{pmatrix} \text{a b c d e} \\ \text{b c d e a} \end{pmatrix} \begin{pmatrix} \text{b c d e a} \\ \text{A D E C B} \end{pmatrix} = \begin{pmatrix} \text{a b c d e} \\ \text{A D E C B} \end{pmatrix}$$

$$Q \rho = \begin{pmatrix} \text{a b c d e} \\ \text{B A D E C} \end{pmatrix} \begin{pmatrix} \text{B A D E C} \\ \text{C B E A D} \end{pmatrix} = \begin{pmatrix} \text{a b c d e} \\ \text{C B E A D} \end{pmatrix}$$

$$\rho^{-1} Q \rho = \begin{pmatrix} \text{a b c d e} \\ \text{e a b c d} \end{pmatrix} \begin{pmatrix} \text{e a b c d} \\ \text{D C B E A} \end{pmatrix} = \begin{pmatrix} \text{a b c d e} \\ \text{D C B E A} \end{pmatrix} .$$

In der Substitutionsschreibweise lauten die Alphabete in diesem Beispiel

i	a b c d e	i	a b c d e	i	a b c d e
0	B A D E C	0	B A D E C	0	B A D E C
1	A D E C B	1	C B E A D	1	D C B E A
2	D E C B A	2	D C A B E	2	B E D C A
3	E C B A D	3	E D B C A	3	B C A E D
4	C B A D E	4	A E C D B	4	E C D B A

In der Zyklenschreibweise erhält man

als Menge der horizontal verschobenen P-Alphabete
{ (a b)(c d e) , (a)(b d c e) , (a d b e)(c) , (a e d)(b c) , (a c)(b)(d)(e)} ,

als Menge der vertikal verschobenen P-Alphabete
{ (a b)(c d e) , (a c e d)(b) , (a d b c)(e) , (a e)(b d c) , (a)(b e)(c)(d)} ,

als Menge der R-rotierten Standardalphabete
{ (a b)(c d e) , (b c)(d e a) , (c d)(e a b) , (d e)(a b c) , (e a)(b c d) } .

Aus der Gruppentheorie weiß man,[1] daß eine Ähnlichkeitstransformation $\rho^{-i}Q\rho^{i}$ die Länge der Einzelzyklen einer Permutation Q invariant läßt. Alle Substitutionen aus der Familie der begleitenden R-rotierten P-Alphabete besitzen also ein und die selbe Zyklenzerlegung. Man hat das den

Hauptsatz der ROTOR-Chiffrierung

genannt.

Für die (horizontal oder vertikal) verschobenen P-Alphabete trifft solches nicht zu.

In unserem Fall ist die Partition, die zu der Zyklenzerlegung gehört, $3+2$. Im Beispiel von 7.2.2 ist die Partition $10+8+6+1+1$, sie gehört zu der Zyklenzerlegung (a n f r l b e o g k) (c w u q j t p h) (d y x v s m) (i) (z) .

7.2.5 Die Anzahl verschiedener verschobener P-Alphabete ist N^n . Die Anzahl verschiedener R-rotierter Alphabete liegt zwischen 1 und N^n , abhängig von R. Für $R = I$, die Identität, beträgt sie 1. Sie beträgt N^n , wenn $\rho^j R \neq R\rho^j$ für $j = 1 , 2 , \ldots , N^n - 1$, denn dann sind alle R-rotierten Alphabete paarweise voneinander verschieden.

Für kleine Werte von N^n gibt es nur wenige Rotoren R , die diese Bedingung erfüllen:

Für $N^n = 4$ und $\rho =$ (a b c d) gibt es vier viergliedrige Rotorfamilien:

{ (a b), (b c), (c d), (d a) } , { (a c b d), (b d c a), (c a d b), (d b a c) } ,
{ (a c b), (b d c), (c a d), (d b a) } , { (a b c), (b c d), (c d a), (d a b) } ;

für $N^n = 3$ und $\rho =$ (a b c) nur eine dreigliedrige: { (a b), (b c), (c a) } .

Für $N^n = 2$ gibt es keine zweigliedrige Rotorfamilie.

[1] siehe etwa *Garrett Birkhoff* und *Saunders MacLane*, A Survey of Modern Algebra, Macmillan, New York 1965, S. 135.

7.3 Rotor-Maschinen

Seit dem Aufkommen elektrischer Schreibmaschinen werden auch elektrische Chiffriergeräte verwendet. Zur elektrischen Kontaktrealisierung einer festen Substitution P dient ein Schaltkasten P mit N Eingangsbuchsen für die Klartextzeichen und N Ausgangsbuchsen für die Geheimtextzeichen, intern verbunden durch N Leitungsdrähte, Abb. 47 (a).

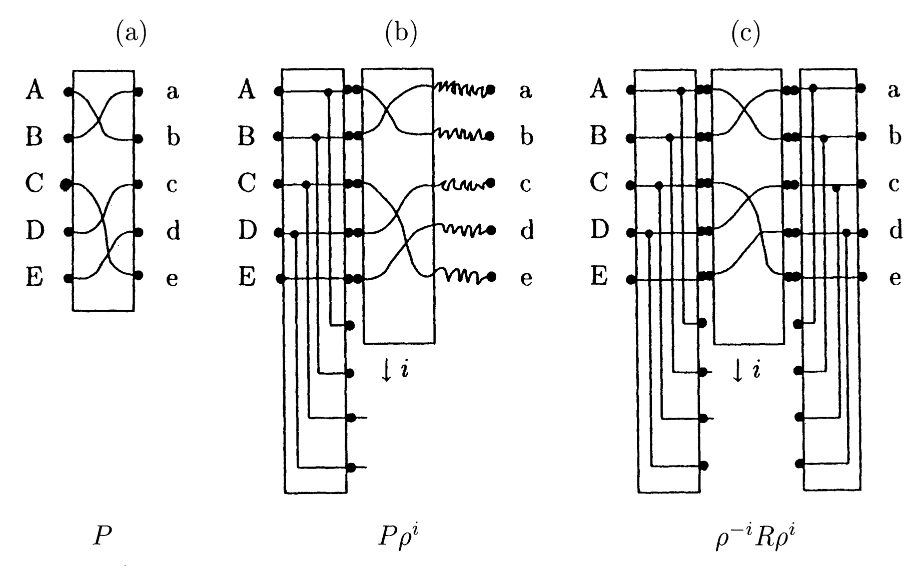


Abb. 47. Feste Permutation, Verschiebung und Rotierung als elektrische Kontaktschaltung

Zum Zwecke einer elektrischen Kontaktrealisierung von begleitenden verschobenen P-Alphabeten $P\rho^i$ kann man hinter die ausgangsseitigen Buchsen des Schaltkastens P eine verschiebbare Kontaktleiste setzen, oder den Schaltkasten P verschiebbar machen, Abb. 47 (b). In jedem Fall muß man flexible Leitungsverbindungen vorsehen, was zu einem Abnutzungsproblem führt.

Dies vermeidet man, wenn man zunächst je eine verschiebbare Kontaktleiste eingangsseitig und ausgangsseitig anbringt und beide starr koppelt. Es ist stattdessen auch möglich, auf flexible Leitungsverbindungen zu verzichten, indem man P verschiebt, Abb. 47 (c). Ohne Duplikation der ein- und ausgangsseitigen Kontakte kommt man aus, wenn man eine drehbare Kontaktscheibe (‚Walze'), einen **Rotor**, benutzt. Man erhält dadurch eine elektrische Kontaktrealisierung von begleitenden, rotierten R-Alphabeten $\rho^{-i}R\rho^i$.

Wenn man allerdings ausgangsseitig Schleifringe benutzt, kann man auch begleitende *verschobene* P-Alphabete $P\rho^i$ elektrisch realisieren. Für diese Anordnung ist der Ausdruck **Halbrotor** gebräuchlich geworden (Abb. 48).

7.3.1 Die Idee des Rotors kommt vor 1920 an vier Stellen unabhängig auf. Folgt man *Kahn*, so geht aus Unterlagen eines Patentstreits hervor, daß

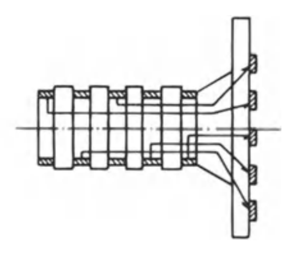



Abb. 48. Halbrotor nach *Arvid Damm*

1917 der Amerikaner *Edward Hugh Hebern* (1869–1952) als erster die Idee hatte; das U.S. Patent (1510441) wurde allerdings erst 1924 erteilt. Dicht auf folgt jedenfalls der Deutsche *Arthur Scherbius* (Patentanmeldung 23. 2. 1918, Deutsches Patent 416 219), später fast im Toten Rennen der Niederländer *Hugo Alexander Koch* (1870–1928), Patentanmeldung 7. 10. 1919 und der Schwede *Arvid Gerhard Damm*, Patentanmeldung 10. 10. 1919.[2] *Damm* verwendete ‚Halbrotoren' mit Schleifringen, die eigentlich verschobene Alphabete nachbilden, paarweise für Polybius-Chiffrierungen. In den Scherbius-Patenten sind auch Rotoren mit 10 Kontakten, geeignet für die Überchiffrierung numerischer Codes, als Beispiele aufgeführt.

Es lag nahe, mehrere Rotoren hintereinanderzuschalten, wie es Scherbius in seiner Patentanmeldung von 1918 vorsah.. *Hebern* verwendete fünf Rotoren (von denen zwei feststehend waren), *Scherbius* in den ersten Modellen ENIGMA A und ENIGMA B vier Rotoren (‚Durchgangsräder'). Im letzteren Fall ergibt sich die Familie $\{R_{(i_1,i_2,i_3,i_4)}\}$ mit

$$R_{(i_1,i_2,i_3,i_4)} = \rho^{-i_1} R_N \rho^{i_1-i_2} R_M \rho^{i_2-i_3} R_L \rho^{i_3-i_4} R_K \rho^{i_4} \quad ,$$

die bei geeigneter Wahl von R_K, R_L, R_M, R_N $26^4 = 456\,976$ Mitglieder hat.

7.3.2 Später, beginnend mit der ENIGMA C von 1926, hatte *Scherbius*' Mitarbeiter *Willi Korn*[3] (Patentanmeldung 21.3.1926, Deutsches Patent 452 194) die anscheinend schlaue Idee, eine Umkehrscheibe[4] einzuführen. Mit drei nunmehr auswechselbaren Rotoren R_L, R_M, R_N und einer echten involutorischen Substitution U (bei geradem N) entsteht die Familie $\{P_{(i_1,i_2,i_3)}\}$, wo

$$P_{(i_1,i_2,i_3)} = S_{(i_1,i_2,i_3)} \, U \, S^{-1}_{(i_1,i_2,i_3)} \quad \text{und}$$
$$S_{(i_1,i_2,i_3)} = \rho^{-i_1} R_N \rho^{i_1-i_2} R_M \rho^{i_2-i_3} R_L \rho^{i_3} \quad .$$

[2] Keinem dieser Erfinder brachte die Erfindung Reichtum und Glück. *Hebern* wurde von der U.S. Regierung sehr schofel behandelt. *Koch* starb schon 1928, nachdem *Scherbius*' Firma seine Patente gekauft hatte. *Scherbius* (30. 10. 1878 – 13. 5. 1929) erlag einem tödlichen Unfall, sein Unternehmen in Berlin firmierte weiterhin als *Heimsoeth & Rinke* bis 1945. *Damm*, der ein *homme galant* war, starb 1928, seine Firma wurde von *Boris Hagelin* (2. 7. 1892 – 7. 9. 1983) übernommen, der die Halbrotoren 1935 aufgab und 1939 die Firma in *Aktiebolaget Ingenjörsfirmen Cryptoteknik* umbenannte.

[3] *Korn* reichte vor 1930 eine Reihe von Patenten ein und gab der ENIGMA viel von ihrer modernen Form. *Korn* meldete noch am 5. März 1930 ein deutsches Patent an, dann verliert sich in Berlin seine Spur.

[4] ‚Umkehrwalze', im Englischen oft *Umkerwaltz* genannt, spaßeshalber auch *Uncle Walter*.

Sämtliche Elemente dieser Familie sind nun echte involutorische Substitutionen. Dies war als Vorteil gedacht, weil zwischen Chiffrierung und Dechiffrierung kein Umschalten erforderlich war; es sollte sich aber als schwerer Nachteil herausstellen (vgl. 11.2.4, 14.5.1, 19.7.2). Der Umstand, daß nunmehr der Stromlauf durch sechs statt durch drei Rotoren ging, wurde auch von einigen Leuten fälschlich als Erhöhung der kryptanalytischen Sicherheit gedeutet — die Ironie des Schicksals wollte es, daß es das Gegenteil war.

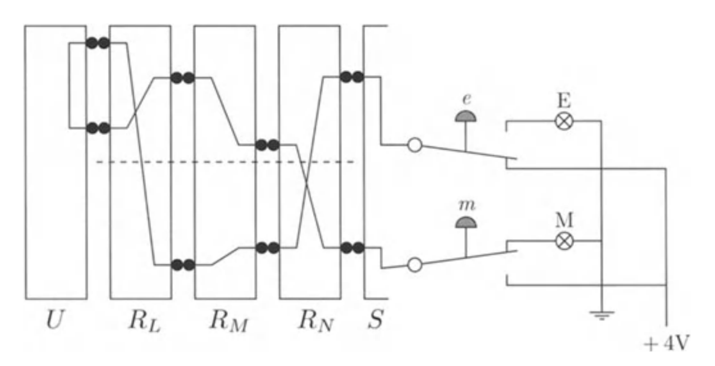


Abb. 49. Stromlauf in einer 3-Rotor-ENIGMA für Taste *e* und Lampe M .

Der Preis einer ENIGMA lag damals bei 600 Reichsmark. Abb. 49 zeigt den Stromlauf der elektrischen Realisierung für das Klartextzeichen e und das zugehörige Geheimtextzeichen M , S bezeichnet die Eingangsscheibe (‚Stator'). Die Umkehrscheibe U konnte in der ENIGMA C in zwei festen Stellungen eingesetzt werden. In der kommerziellen ENIGMA D von 1927 wurde sie wie die drei Rotoren einstellbar gemacht, sie sah wie ein viertes Durchgangsrad aus (‚Umkehrwalze' im engeren Sinn), wurde aber nicht mitbewegt.

So entsteht die Familie $\{P_{(i_1,i_2,i_3,i_4)}\}$ von echten Involutionen, wo

$$P_{(i_1,i_2,i_3,i_4)} = S_{(i_1,i_2,i_3,i_4)} \; U \; S^{-1}_{(i_1,i_2,i_3,i_4)} \quad \text{und}$$
$$S_{(i_1,i_2,i_3,i_4)} = \rho^{-i_1} R_N \, \rho^{i_1-i_2} R_M \, \rho^{i_2-i_3} R_L \, \rho^{i_3-i_4} \quad .$$

Die erstmals mit Reservewalzen ausgestattete ENIGMA D war weitverbreitet, sie ging nach Schweden, den Niederlanden, England, Japan, Italien, Spanien, U.S.A und wurde vom polnischen Chiffrierbüro legal gekauft. Sie wurde auch, wie ihr Nachfolgemodell ENIGMA K, 1938–1940 an die Schweizer Armee verkauft (von den Amerikanern INDIGO genannt). In den späteren Modellen für die Reichswehr, ab 1930, war die Umkehrwalze wieder fest ($i_4 = 0$).

Der polnische Chiffrierdienst (*Biuro Szyfrów*) fing bereits am 15. Juli 1928 ENIGMA-chiffrierte Funksprüche auf. Die Reichsmarine experimentierte seit 1925 mit einer 3-Rotor-ENIGMA („Funkschlüssel C" von 1926), die 28 Kontakte aufwies; ihr alphabetisch angeordnetes Tastenfeld hatte die zusätzlichen Zeichen Ä, Ö, Ü, wobei X unchiffriert blieb. Die Umkehrwalze konnte jetzt in vier festen Stellungen, mit $\alpha, \beta, \gamma, \delta$ bezeichnet, eingesetzt werden. Um 1933 war auch eine Version des Funkschlüssel C mit 28 Alphabetzeichen

(zusätzlich: Ä, Ü) in Erprobung. 1933 traten geringfügige Änderungen im Funkschlüssel C in Kraft. In den Reichswehr-Modellen ENIGMA G (im Heer eingeführt am 15. 7. 1928) und ENIGMA I (1930) waren wieder 26 Kontakte vorhanden und ein Tastenfeld, das bis auf die Lage des Buchstabens P der gewöhnlichen Schreibmaschinetastatur entsprach. Die Verbindung zu den Kontakten des Stators folgte der alphabetischen Ordnung. Die Umkehrwalze konnte nur in *einer* Stellung eingesetzt werden. Es gab auch eine ENIGMA II mit einem Schreibwerk, sie wurde als unpraktisch erachtet und wenig benutzt.

Die am 1. Juni 1930 eingeführte ENIGMA I (‚eins') des Heeres, die später zur gemeinsamen ‚Wehrmachts-ENIGMA' wurde, war durch ein zusätzliches ‚Steckerbrett' gesichert, das eine feste vorgeschaltete (unnötigerweise involutorische) Substitution T, die **Steckerverbindung**, erlaubte. Dies ergibt die

ENIGMA-Gleichung $c_i = p_i \; T \; S_i \; U \; S_i^{-1} \; T^{-1} \quad (= \; p_i \; T \; P_i \; T^{-1} \;) \,,$

ein Zusammenhang zwischen Klartextzeichen p_i und Geheimtextzeichen c_i. Nach 2.6.3 sind $c_i \, T S_i$ und $p_i \, T S_i \, U$ isomorph: Es ist $c_i \, T S_i = p_i \, T S_i \; U$.

7.3.3 1934 einigten sich Kriegsmarine und Heer unter dem Druck von Oberst *Erich Fellgiebel* (1886–1944), später (ab 1939) Generalmajor und Chef des Wehrmacht-Nachrichtenverbindungswesens, zugleich Chef des Heeresnachrichtenwesens, auf eine gemeinsame Version (Abb. 50a). Die drei auswechselbaren Rotoren zeigt Abb. 50b.

Für die Marine-ENIGMA (‚Funkschlüssel M') konnten die drei Rotoren ab 1934, 1938, 1939 aus einem Satz von 5, 7 bzw. 8 Rotoren ausgewählt (und außerdem permutiert) werden. Sie waren mit den römischen Ziffern I bis VIII numeriert. Das Heer gab bis 15. 12. 1938 nur drei der vorgesehenen fünf Rotoren zur Benutzung frei. Auch die Luftwaffe führte 1935 für ihre ‚Luftnachrichtentruppe' die Wehrmachts-ENIGMA ein.

Die Deutsche Reichsbahn, die Reichspost und die Polizei benutzten weniger sichere ältere Modelle ohne Steckerbrett, obwohl etwa Nachrichten über Eisenbahntransporte in Rußland für den Feind sehr aufschlußreich waren.

Die mit ‚A' bezeichnete Umkehrwalze der Wehrmachts-ENIGMA wurde am 1. 11. 1937 durch eine Umkehrwalze ‚B' ersetzt. 1941 wurde eine Umkehrwalze ‚C' eingeführt, eine Umkehrwalze ‚D' mit variabler Verdrahtung trat erstmals am 2. Januar 1944 im Funkverkehr mit Norwegen auf. Die Verdrahtung wurde häufig geändert (Abb. 51b).

Die einzelnen Rotoren konnten in beliebiger Reihenfolge in die ENIGMA eingesetzt werden. Bis Ende 1935 war diese ‚Walzenlage' und die Steckerverbindung für drei Monate fest. Ab 1. 1. 1936 wechselten sie alle Monate, ab 1. 10. 1936 jeden Tag. Später im 2. Weltkrieg, ab Mitte 1942, wurden sie alle 8 Stunden gewechselt. Man fragt sich, warum nicht früher?

Die Kriegsmarine war stets in Sorge um die Chiffriersicherheit der ENIGMA. Am 1. 2. 1942 wurde eine Version M4 der Marine-ENIGMA mit einem vierten Rotor (‚Griechenwalze') β eingeführt (Farbtafel I) und zunächst nur von

Abb. 50a. 3-Rotor-ENIGMA der *Wehrmacht* (1937)

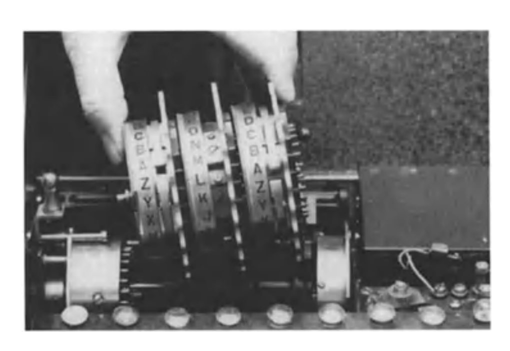


Abb. 50b. Die drei auswechselbaren Rotoren der Wehrmachts-ENIGMA (1937)

den Atlantik-U-Booten (Schlüsselnetz ‚Triton') benutzt; dieser Rotor wurde während der Chiffrierung nicht fortbewegt. Am 1. 7. 1943 wurde ein weiterer Rotor γ eingeführt. Um die Verträglichkeit der 4-Rotor-ENIGMA mit der 3-Rotor-ENIGMA zu gewährleisten, wurde deren Umkehrwalze aufgespalten in eine ‚dünne Umkehrscheibe' ‚B dünn' oder ‚C dünn' und den fest einstellbaren zusätzlichen Rotor β oder γ. Eine Aufspaltung der nicht mehr verwendeten Umkehrwalze ‚A' erübrigte sich.[5]

Eine andere Erfindung, die *Paul Bernstein* schon für die ENIGMA A machte, wurde kein kryptologischer Reinfall: Der Ring, auf dem die Rotoreinstellung abgelesen werden konnte (‚Sperr-Ring') war verstellbar, die **Ringstellung** (engl. *ring setting, core-position*) konnte mit einem Stift fixiert werden.

Abb. 51a zeigt ein Blatt aus der Dienstvorschrift für die ENIGMA der Wehrmacht mit den täglich wechselnden Walzenlagen, Ringstellungen und Steckerverbindungen (‚Tagesschlüssel'). Die Grundstellung kennzeichnete die Einstellung der drei Rotoren zu Beginn eines Spruches. Die Kenngruppen hatten keine kryptologische Bedeutung. Abb. 51b zeigt Schlüsselunterlagen der Luftwaffe aus dem Jahr 1944, aus denen hervorgeht daß die Verdrahtung der Umkehrwalze ‚D' alle 10 Tage und einige Steckerverbindungen alle 8 Stunden geändert wurden. Es gab zuletzt dafür auch eine ‚Uhr' (Farbtafel M).

ENIGMAs wurden beim Heer vom Regiment an aufwärts eingesetzt. Nach einer hohen Schätzung (*Johnson*) wurden insgesamt 200 000, nach einer niedrigen polnischen waren bereits 1938 mindestens 20 000 ENIGMAs in Gebrauch und bis Kriegsausbruch mindestens 40 000 . Knapp 100 000 dürfte richtig sein. Nach dem 2. Weltkrieg verkauften die Siegermächte erbeutete ENIGMA-Maschinen, die damals weithin noch als sicher galten, an Entwicklungsländer.

7.3.4 Rotor-Maschinen wurden im 2. Weltkrieg auch in England gebaut. Die Maschine TYPEX war eine Fortentwicklung der ENIGMA, sie hatte u. a. eine Eingangs-Substitution, die nicht involutorisch war (s. 22.2.7). In den USA gab es unter dem Einfluß von *William Friedman* (1891–1969) und aufbauend auf den Arbeiten von *Hebern* in den frühen dreißiger Jahren eine unabhängige Linie von Rotor-Maschinen, die 1933 zur M-134-T2, sodann zur M-134-A (SIGMYC) und schließlich 1936 zur M-134-C (SIGABA) $\hat{=}$ CSP889 (ECM Mark II) führte. Es gelang den Deutschen offenbar kein Einbruch in die von *William Friedman* entworfene SIGABA, die von *Frank Rowlett* (1908–1998), der seit April 1930 sein Gehilfe war, wasserdicht gemacht worden war.

Eine interessante Nachkriegsvariante der ENIGMA mit sieben Rotoren und einer festen Umkehrscheibe wurde von der italienischen Firma *Ottico Meccanica Italiana* (OMI) in Rom gebaut und vertrieben. Die Schweizer Armee benutzte ab 1946 eine von Zellweger A.G., Uster gebaute ENIGMA-Variante NEMA mit zehn Walzen, von denen jedoch nur sechs zur Chiffrierung dienten, die übrigen lediglich zur unregelmäßigen Fortschaltung.

---

[5] *J. Rohwer* erwähnte 1978 eine Griechenwalze α , *Deavours* und *Kruh* (1985) folgten ihm. Dazu *D. Kahn*: "No α rotor was ever recovered". In der Tat: an eine Aufspaltung der Umkehrwalze ‚A', die 1937 aufgegeben worden war, zu denken, ergibt keinen Sinn.

VIII. Beispiel.

17. Gültiger Tagesschlüssel:

(Ausschnitt aus der für die Verschlüsselung des Klartextes in Betracht kommenden Schlüsseltafel, z. B. »........... Maschinenschlüssel für Monat Mai«)

Datum	Walzenlage	Ringstellung	Grundstellung
4.	I III II	16 11 13	01 12 22

Steckerverbindung	Kenngruppen-Einsatzstelle ...... Gruppe	Kenngruppen
CO DI FR HU JW LS TX	2	adq nuz opw vxz

Abb. 51a. Aus der Wehrmacht-Dienstvorschrift für die ENIGMA, datiert 8. Juli 1937. Die Einstellung der Ringstellung und der Walzenlage war einem Offizier vorbehalten.

N° 000082

Luftwaffen-Maschinen-Schlüssel Nr. 2744

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

Monats-Tag	Walzenlage			Ringstellung			an der Umkehrwalze	Steckerverbindungen am Steckerbrett 1	2	3	4	5	6	7	8	9	10	Zusatzsteckerverbindungen 1 (1500)	2 (2300)	Kenngruppen			
31	III	V	IV	17	11	04	HX GL NQ SV UX TZ / RW AD BP CO EP IM	TW	BI	UY	GP	CK	JQ	DL	RV	EM	AH	NS	FO	kim	pwh	sbx	osw
30	I	IV	V	08	17	21		LS	DH	MT	EO	AP	UZ	FQ	WY	BK	GR	CI	JN	uaq	omn	ume	duf
29	V	II	III	11	14	05		DO	JW	CN	IV	PZ	BM	HU	AL	FR	KX	EQ	GT	don	cqo	xum	bpg
28	II	IV	V	02	20	16		NT	HK	BW	EP	LQ	AU	OY	FJ	CX	GI	DZ	MR	lui	pyg	sby	dtq
27	III	V	IV	18	13	22		HM	GV	KZ	AI	DQ	NR	ES	BL	OU	FT	CP	JY	cmy	fqr	scl	bur
26	I	III	II	24	10	01		GW	AQ	MO	FV	PS	DI	RU	JZ	BN	EH	KT	CL	kbj	yaq	udm	cnz
25	IV	I	III	04	25	23		LT	DR	QX	AG	IN	EU	BJ	KP	FW	CM	SZ	HO	kqz	yar	vdb	cea
24	V	III	I	09	19	06		GL	MY	CR	HN	JX	DT	AF	PU	IQ	BO	EW	KS	cms	aej	sed	auh
23	IV	I	V	15	03	19		IT	DV	HQ	AJ	MU	EX	KO	CS	FY	LN	BP	GZ	kra	yas	xun	ceb
22	I	V	III	12	26	07		EY	JL	AK	NV	FZ	CT	HP	MX	BQ	GS	DW	IO	jdm	uhf	xuo	bph
21	III	IV	II	15	09	12	AG IR BH CS DZ EW / FK LX MP OU NT QV	JP	DY	QS	HL	AE	NW	CU	IK	FX	BR	MV	GO	jpf	aok	iys	btx
20	IV	II	I	02	22	05		HT	NP	AM	DX	GJ	KQ	BS	OV	ER	CW	IU	PL	boy	wac	uow	cse
19	V	I	II	08	19	17		GM	OX	BT	QU	DP	HJ	FK	SW	AN	EL	CY	IR	xjc	wad	unj	ctd
18	III	IV	I	11	21	01		KW	IP	DM	SV	JR	CX	EN	AZ	QT	BU	FH	GY	kpn	rzi	vcm	bpo
17	I	V	II	18	23	14		BV	HW	AR	NX	DS	PT	CZ	FI	LY	EJ	GK	MQ	kdx	crq	vcn	cod
16	III	IV	V	16	04	07		LU	CV	FM	KR	BY	GN	QW	DJ	PS	AO	EI	HX	lgx	jri	uob	aur
15	V	III	IV	24	13	10		HZ	NQ	AD	TV	IX	KM	BG	LO	CE	RY	JU	FP	wpt	vhy	zoe	aus
14	I	IV	II	06	20	25		FN	UY	CJ	IW	LP	AS	DK	GQ	MO	BZ	ET	HR	wog	hxi	zxi	bpi
13	III	II	I	03	26	18		KR	IZ	AT	NV	BH	MP	CG	OY	ES	DF	UW	LQ	lqv	iqb	zsy	coe
12	II	IV	III	04	11	15		DT	JV	HS	CI	AY	KU	EN	FQ	LR	BW	MP	GO	zic	myt	zof	dtr
11	V	I	IV	16	07	02		JS	PW	AV	QX	DN	IZ	KM	CO	EG	FL	HY	BR	inf	zbm	krz	dug
10	IV	III	II	20	12	14		FS	CQ	JO	PR	AW	HV	EZ	KN	DU	GT	IL	BY	ink	acu	zxj	cnu
9	III	II	V	06	18	10	HL KN FM EI AC BG / DS OW PZ QX RU TV	HK	TZ	MX	LW	GQ	AD	NY	BE	CS	JP	RV	IO	efm	pmi	snw	cof
8	V	I	III	01	21	17		GU	SW	BF	RX	EV	OT	LQ	CH	IP	KY	JM	NZ	imy	rjw	tjm	cog
7	II	V	I	25	08	23		CX	AZ	DV	KT	HU	LW	GP	EY	MR	FQ	IN	OS	inv	rkc	snx	bpj
6	IV	II	V	13	26	03		DV	LP	NQ	GZ	OS	FK	EW	MR	IT	HX	UY	BJ	yvu	hsb	swq	aut
5	III	I	II	24	19	22		SY	EK	NZ	OR	CG	JM	QU	PV	BI	LW	TX	DF	seu	iqe	swr	auv
4	II	IV	I	17	05	09		BD	GV	AX	KP	EM	FN	CW	RU	HO	JT	IL	QS	zfj	hxj	zxk	dpt
3	V	II	IV	20	16	11		JT	NW	DU	EO	KV	BY	FS	HQ	IM	LX	GP	CR	clx	zbn	zxa	buk
2	II	III	V	14	03	19		RW	OQ	GI	AZ	EJ	MS	CU	DH	PY	BF	LV	TX	ljs	jre	zpq	coh
1	III	I	IV	18	24	15		NP	JV	LY	IX	KQ	AO	DZ	CR	FT	EM	GS	HW	plf	dgw	tjn	cnv

Fig. 51b. Schlüsselunterlagen *nr 2744* für *Luftwaffen*-ENIGMA (1944)

7.3.5 Die Substitutionen des Stators, der drei Rotoren und der Umkehrwalze der ENIGMA D sind (*Cipher A. Devours*, *Louis Kruh*):

Eingang	a b c d e f g h i j k l m n o p q r s t u v w x y z
Stator	J W U L C M N O H P Q Z Y X I R A D K E G V B T S F
Rotor 1	L P G S Z M H A E O Q K V X R F Y B U T N I C J D W
Rotor 2	S L V G B T F X J Q O H E W I R Z Y A M K P C N D U
Rotor 3	C J G D P S H K T U R A W Z X F M Y N Q O B V L I E
Umkehrwalze	I M E T C G F R A Y S Q B Z X W L H K D V U P O J N

Die Substitutionen des Stators, der acht Rotoren und der beiden Umkehrwalzen der Wehrmachts-ENIGMA sind (*Ralph Erskine*, *Frode Weierud*, *Philip Marks*, *Heinz Ulbricht*):

Eingang		a b c d e f g h i j k l m n o p q r s t u v w x y z
Stator		A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Rotor	I	E K M F L G D Q V Z N T O W Y H X U S P A I B R C J
Rotor	II	A J D K S I R U X B L H W T M C Q G Z N P Y F V O E
Rotor	III	B D F H J L C P R T X V Z N Y E I W G A K M U S Q O
Rotor	IV	E S O V P Z J A Y Q U I R H X L N F T G K D C M W B
Rotor	V	V Z B R G I T Y U P S D N H L X A W M J Q O F E C K
Rotor	VI	J P G V O U M F Y Q B E N H Z R D K A S X L I C T W
Rotor	VII	N Z J H G R C X M Y S W B O U F A I V L P E K Q D T
Rotor	VIII	F K Q H T L X O C B J S P D Z R A M E W N I U Y G V
Umkehrwalze	A	E J M Z A L Y X V B W F C R Q U O N T S P I K H G D
Umkehrwalze	B	Y R U H Q S L D P X N G O K M I E B F Z C W V J A T
Umkehrwalze	C	F V P J I A O Y E D R Z X W G C T K U Q S B N M H L
Rotor	Beta	L E Y J V C N I X W P B Q M D R T A K Z G F U H O S
Umkehrwalze	B dünn	E N K Q A U Y W J I C O P B L M D X Z V F T H R G S
Rotor	Gamma	F S O K A N U E R H M B T I Y C W L Q P Z X V G J D
Umkehrwalze	C dünn	R D O B J N T K V E H M L F C W Z A X G Y I P S U Q

Beachte: Beta, gefolgt von B dünn, gefolgt von Beta^{-1}, ergibt B, beispielsweise $\text{Beta}(a) = \text{L}$, $\text{B dünn}(\text{L}) = \text{O}$, $\text{Beta}^{-1}(\text{O}) = \text{y}$, also $\text{B}(a)=\text{y}$.

Die Substitutionen des Stators, der drei Rotoren und der Umkehrwalze der Reichsbahn-ENIGMA sind (*David H. Hamer*, *Geoff Sullivan*, *Frode Weierud*):

Eingang		a b c d e f g h i j k l m n o p q r s t u v w x y z
Stator		Q W E R T Z U I O A S D F G H J K P Y X C V B N M L
Rotor	I	J G D Q O X U S C A M I F R V T P N E W K B L Z Y H
Rotor	II	N T Z P S F B O K M W R C J D I V L A E Y U X H G Q
Rotor	III	J V I U B H T C D Y A K E Q Z P O S G X N R M W F L
Umkehrwalze		Q Y H O G N E C V P U Z T F D J A X W M K I S R B L

Die Substitutionen des Stators, der drei Rotoren und der Umkehrwalze der Schweizer ENIGMA K sind (*David H. Hamer*, *Geoff Sullivan*, *Frode Weierud*):

Eingang		a b c d e f g h i j k l m n o p q r s t u v w x y z
Stator		Q W E R T Z U I O A S D F G H J K P Y X C V B N M L
Rotor	I	P E Z U O H X S C V F M T B G L R I N Q J W A Y D K
Rotor	II	Z O U E S Y D K F W P C I Q X H M V B L G N J R A T
Rotor	III	E H R V X G A O B Q U S I M Z F L Y N W K T P D J C
Umkehrwalze		I M E T C G F R A Y S Q B Z X W L H K D V U P O J N

Die Substitutionen des Stators, der drei Rotoren und der Umkehrwalze der Abwehr-ENIGMA (Nr. G-312) sind (*David H. Hamer*):

Eingang		a b c d e f g h i j k l m n o p q r s t u v w x y z
Stator		Q W E R T Z U I O A S D F G H J K P Y X C V B N M L
Rotor	I	D M T W S I L R U Y Q N K F E J Z A Z B P G X O H V
Rotor	II	H Q Z G P J T M O B L N C I F D Y A W V E U S R K X
Rotor	III	U Q N T L S Z F M R E H D P X K I B V Y G J C W O A
Umkehrwalze		R U L Q M Z J S Y G O C E T K W D A H N B X P V I F

Die Rotoren der ENIGMA D und der Wehrmachts-ENIGMA weisen folgende Zyklenzerlegungen der Substitutionen auf, die die Identifizierung erleichtern:

Stator	13+7+3+2+1	Rotor I	10+4+4+3+2+2+1
Rotor 1	25+1	Rotor II	8+7+3+2+2+2+1+1
Rotor 2	17+7+2	Rotor III	17+8+1
Rotor 3	19+6+1	Rotor IV	22+2+2
		Rotor V	11+9+6
		Rotor VI	14+8+4
		Rotor VII	26
		Rotor VIII	17+3+3+3

Rotor I der Wehrmachts-ENIGMA ergibt die folgenden rotierten Alphabete (mit Ringstellung A für $i = 0$):

Ringstellung	i	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	0	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
Z	1	K	F	L	N	G	M	H	E	R	W	A	O	U	P	X	Z	I	Y	V	T	Q	B	J	C	S	D
Y	2	E	L	G	M	O	H	N	I	F	S	X	B	P	V	Q	Y	A	J	Z	W	U	R	C	K	D	T
X	3	U	F	M	H	N	P	I	O	J	G	T	Y	C	Q	W	R	Z	B	K	A	X	V	S	D	L	E
W	4	F	V	G	N	I	O	Q	J	P	K	H	U	Z	D	R	X	S	A	C	L	B	Y	W	T	E	M
V	5	N	G	W	H	O	J	P	R	K	Q	L	I	V	A	E	S	Y	T	B	D	M	C	Z	X	U	F
U	6	G	O	H	X	I	P	K	Q	S	L	R	M	J	W	B	F	T	Z	U	C	E	N	D	A	Y	V
T	7	W	H	P	I	Y	J	Q	L	R	T	M	S	N	K	X	C	G	U	A	V	D	F	O	E	B	Z
S	8	A	X	I	Q	J	Z	K	R	M	S	U	N	T	O	L	Y	D	H	V	B	W	E	G	P	F	C
R	9	D	B	Y	J	R	K	A	L	S	N	T	V	O	U	P	M	Z	E	I	W	C	X	F	H	Q	G
Q	10	H	E	C	Z	K	S	L	B	M	Z	O	U	W	P	V	Q	N	A	F	J	X	D	Y	G	I	R
P	11	S	I	F	D	A	L	T	M	C	N	U	P	V	X	Q	W	R	O	B	G	K	Y	E	Z	H	J
O	12	K	T	J	G	E	B	M	U	N	D	O	V	Q	W	Y	R	X	S	P	C	H	L	Z	F	A	I
N	13	J	L	U	K	H	F	C	N	V	O	E	P	W	R	X	Z	S	Y	T	Q	D	I	M	A	G	B
M	14	C	K	M	V	L	I	G	D	O	W	P	F	Q	X	S	Y	A	T	Z	U	R	E	J	N	B	H
L	15	I	D	L	N	W	M	J	H	E	P	X	Q	G	R	Y	T	Z	B	U	A	V	S	F	K	O	C
K	16	D	J	E	M	O	X	N	K	I	F	Q	Y	R	H	S	Z	U	A	C	V	B	W	T	G	L	P
J	17	Q	E	K	F	N	P	Y	O	L	J	G	R	Z	S	I	T	A	V	B	D	W	C	X	U	H	M
I	18	N	R	F	L	G	O	Q	Z	P	M	K	H	S	A	T	J	U	B	W	C	E	X	D	Y	V	I
H	19	J	O	S	G	M	H	P	R	A	Q	N	L	I	T	B	U	K	V	C	X	D	F	Y	E	Z	W
G	20	X	K	P	T	H	N	I	Q	S	B	R	O	M	J	U	C	V	L	W	D	Y	E	G	Z	F	A
F	21	B	Y	L	Q	U	I	O	J	R	T	C	S	P	N	K	V	D	W	M	X	E	Z	F	H	A	G
E	22	H	C	Z	M	R	V	J	P	K	S	U	D	T	Q	O	L	W	E	X	N	Y	F	A	G	I	B
D	23	C	I	D	A	N	S	W	K	Q	L	T	V	E	U	R	P	M	X	F	Y	O	Z	G	B	H	J
C	24	K	D	J	E	B	O	T	X	L	R	M	U	W	F	V	S	Q	N	Y	G	Z	P	A	H	C	I
B	25	J	L	E	K	F	C	P	U	Y	M	S	N	V	X	G	W	T	R	O	Z	H	A	Q	B	I	D



Edward Hugh Hebern



Arvid Gerhard Damm



Arthur Scherbius

7.4 Verschobene Standardalphabete: Vigenère und Beaufort

Wählt man in 7.2.1 a′) $P = \rho$, so gelangt man zu $\{ \rho^i \rho : i \in \mathbb{N} \}$, der Menge der horizontal verschobenen Standardalphabete, die aber, vgl. 7.2.1 a″), mit $\{\rho \rho^i : i \in \mathbb{N} \}$, der Menge der vertikal verschobenen und überdies mit $\{\rho^i : i \in \mathbb{N} \}$, der Menge der potenzierten Standardalphabete, übereinstimmt. Zur Mechanisierung dieses Falles, der von dem Benediktinerabt *Johannes Heidenberg* aus Trittenheim an der Mosel, genannt *Trithemius* (1462–1516), im 5. Buch seiner *Polygraphiae* nur in Form einer *Tabelle* (‘*tabula recta*’, Abb. 52) behandelt wurde, kann also eine *Alberti*sche Scheibe, die auch innen das Standardalphabet trägt, benutzt werden; aber auch, da es sich um eine reine Potenzierung handelt, eine Scheibe mit dem Zyklus ρ des Standardalphabets und einem beweglichen Fenster. Die Literatur spricht in diesem speziellen Fall von VIGENÈRE-**Chiffrierschritten**. Eigentlich müßte dieser triviale Fall nach *Trithemius* benannt werden.

Die Sekundärliteratur des 19. Jahrhunderts tat *Vigenère* insofern Unrecht, als sie nur die verschobenen *Standard*alphabete mit seinem Namen belegte. *Vigenère* schrieb in die Kopfzeile der *tabula recta* ein permutiertes Alphabet,was gleichwertig war mit *Alberti*s Scheibe, s. 8.1.

Die Menge $\{ \rho^i : i \in \mathbb{N} \}$ wird (Abb. 48) elektrisch durch einen Halbrotor wiedergegeben.

7.4.1 Ein VIGENÈRE-Chiffrierschritt bewirkt offensichtlich eine einfache lineare Substitution: Der Zyklus ρ legt als zyklische lineare Ordnung von V^n die Addition *modulo* N^n fest (5. Kapitel); einem Chiffrierschritt $\rho^i : i \in \mathbb{N}$ entspricht[6] die Addition $A_i : i \in \mathbb{Z}_{N^n}$ einer Verschiebungszahl i:

$$A_i : A_i(x) \overset{N^n}{\simeq} x + i \ .$$

Der Dechiffrierschritt A_i^{-1} bedeutet eine Subtraktion der Verschiebungszahl:

$$A_i^{-1} : A_i^{-1}(y) \overset{N^n}{\simeq} y - i \ .$$

Als LARRABEE bezeichnete man im State Department und in der U.S. Army ein ab 1913 (unter Präsident *Wilson*) eingeführtes Vigenère-Verfahren, bei dem 26 Karten, für jeden Schlüsselbuchstaben eine, jeweils das Klartextalphabet und das zugehörige (verschobene) Geheimtextalphabet enthielten.

7.4.2 Multiplikation mit einem regulären Faktor q ergibt auch eine Familie $\{ C_q : q \in \mathbb{Z}_{N^n} \wedge ggt(q, N^n) = 1 \}$, die der EYRAUD-**Chiffrierschritte**:

$$C_q : C_q(x) \overset{N^n}{\simeq} q \cdot x \ .$$

Der Dechiffrierschritt ist

$$C_q^{-1} : C_q^{-1}(x) \overset{N^n}{\simeq} q' \cdot x \ , \quad \text{wo} \quad q \cdot q' \overset{N^n}{\simeq} 1 \ \ \text{(siehe Tab. 1).}$$

[6] Solche ‘*cryptographic equations*’ hatte schon *Babbage*, ab etwa 1846, benutzt, aber nicht veröffentlicht. (British Museum, Add. Ms. 37205, Folio 59)

Recta transpositionis tabula.

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w
b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a
c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b
d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c
e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d
f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e
g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f
h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g
i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h
k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i
l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k
m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l
n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m
o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n
p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o
q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p
r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q
s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r
t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s
u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t
x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u
y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x
z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y
w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z

Abb. 52. '*tabula recta*' des *Trithemius*. Aus der *Polygraphiae* (1508-1518), 5. Buch (Original in der Bayerischen Staatsbibliothek München

Es handelt sich hier im nichttrivialen Falle $|\,q\,| \neq 1$ um ein **dezimiertes Standardalphabet** (frz. *alphabet chevauchant*, *Eyraud*), vgl. 5.6.

Im Ring $\mathbb{Z}_{N^n}$ lautet die allgemeinste lineare Substitution

$$T_{q,i}: \ T_{q,i}(x) \overset{N^n}{\simeq} q \cdot x + i \ .$$[7]

7.4.3 Der Fall, daß q fest und zwar gleich $N^n - 1$ gewählt wird, ergibt die Familie $\{ B_i : i \in \mathbb{Z}_{N^n} \}$ mit

$$B_i: \ B_i(x) \overset{N^n}{\simeq} i - x \ .$$

[7] *Eyraud* gibt ein Verfahren an, das zu je einem klartextseitigen und geheimtextseitigen Standardalphabet nach zulässiger Wahl von q und q' eine Familie von Chiffrierschritten und Dechiffrierschritten gibt: Man schreibt das eine Alphabet in Zeilen zu q, das andere zu q' Elementen periodisch fortgesetzt, und liest sodann, von einer festzulegenden Anfangspaarung ausgehend, zeilenweise im Klar- und spaltenweise im Geheimtextblock, um den Chiffrierschritt zu erhalten — oder auch zeilenweise im Geheim- und spaltenweise im Klartextblock, um den Dechiffrierschritt zu erhalten.

Beispiel: $n = 1$, $N^n = 26$, $q = 3$, $q' = 9$; Anfangspaarung: **c** – **P** .

Klaralphabet	e v i t z l s **c** o u r a n d b f g h j k m p q w x y
Chiffrenalphabet	S E C U R I T Y A B D F G H J K L M N O **P** Q V W X Z

Die Literatur spricht in diesem Fall von BEAUFORT-**Chiffrierschritten**.[8] Der Dechiffrierschritt

$$B_i^{-1}:\quad B_i^{-1}(y) \overset{N^n}{\simeq} i - y$$

fällt mit dem Chiffrierschritt zusammen, der BEAUFORT-Chiffrierschritt ist involutorisch, aber nicht echt involutorisch:

$$x \text{ ist Fixpunkt von } B_i \text{ genau dann wenn } 2 \cdot x \overset{N^n}{\simeq} i\ .$$

Im klassischen Fall (vgl. 5.5) ist natürlich $n = 1$. Übrigens hat erst *de Viaris*, der ein mathematischer Kopf war[9], 1888 die Deutung des VIGENÈRE-Chiffrierschritts als Addition *modulo N* publiziert, nachdem schon *Kerckhoffs* 1883 (ohne von den Vorarbeiten von *Babbage* zu wissen) die mathematischen Beziehungen zwischen VIGENÈRE und BEAUFORT aufgezeigt hatte. Vorher und teilweise noch nachher half man sich mit den Erklärungen dieser Prozesse durch die auch in der Praxis als Geräte dienenden Saint-Cyr-Schieber (*cipher slide*, *réglette à chiffrer*, 3.2.7).

Mit fester Schiebereinstellung wird ein VIGENÈRE-Chiffrierschritt zu einem CAESAR-Chiffrierschritt, ein BEAUFORT-Chiffrierschritt wird zu einem CAESAR-Chiffrierschritt am revertierten Alphabet.

e v i	S E C U R I T Y A
t z l	B D F G H J K L M
s **c** o	N O **P** Q V W X Z S
u r a	E C **U** R I T Y A B
n d b	D F **G** H J K L M N
f g h	O P **Q** V W X Z S E
j k m	C U **R** I T Y A B D
p q w	F G **H** J K L M N O
x y e	P Q **V** W X Z S E C
v i t	U R **I** T Y A B D F
z l s	G H **J** K L M N O P
⋮	⋮

e v i	S E C U R I T Y A
t z l	B D F G H J K L M
s **c** o	N O **P** Q V W X Z S
u **r** a	E C U R I T Y A B
n **d** b	D F G H J K L M N
f **g** h	O P Q V W X Z S E
j **k** m	C U R I T Y A B D
p **q** w	F G H J K L M N O
x **y** e	P Q V W X Z S E C
v **i** t	U R I T Y A B D F
z **l** s	G H J K L M N O P
⋮	⋮

Chiffrierschritt

c o u r a n d b f g h j k m p q w x y e v i t z l s
P U G Q R H V I J W T K X Y L Z A M S B N E D O C F

Dechiffrierschritt

P Q V W X Z S E C U R I T Y A B D F G H J K L M N O
c r d g k q y i l o a b h m w e t s u n f j p x v z

in Zyklenschreibweise

(a r q z o u g w)(b e i)(c p l)(d v n h t)(f j k x m y s) .

[8] Schon von *Giovanni Sestri* 1710 betrachtet, von Admiral *Sir Francis Beaufort* (1774–1857, besser bekannt von den Windstärken her) 1857 wiederentdeckt. Für die in der englischen Literatur als '*variant Beaufort*', in der französischen Literatur als '*variante à l'allemande*' bezeichnete Variante, die 1858 unabhängig *Lewis Carroll* alias *Charles Lutwidge Dodgson* vorschlug, siehe 7.4.4.

[9] *Marquis Gaëtan Henri Léon de Viaris*, 1847–1901, französischer Offizier. *De Viaris* erfand auch um 1885 eine der ersten druckenden Chiffriermaschinen — die allererste erfanden nach *Kahn* vermutlich vor 1874 *Émile Vinay* und *Joseph Gaussin*.

7.4.4 Eine triviale Variante der VIGENÈRE-Chiffrierung

$$E_i : \quad E_i(x) \overset{N^n}{\simeq} -i + x$$

wird in der Literatur als ‚Rückwärts'-VIGENÈRE (engl. *'Variant Beaufort'*, frz. *'variante à l'allemande'*) bezeichnet.

Die ebenfalls schon von *de Viaris* diskutierte involutorische Variante der BEAUFORT-Chiffrierung

$$F_i : \quad F_i(x) \overset{N^n}{\simeq} -i - x$$

wurde 1972 von *Ole Immanuel Franksen* wiederentdeckt.

Eine ‚Variante', unter dem Stichwort GRONSFELD[10] laufend, ist gar keine – es ist VIGENÈRE, wobei nur zehn Alphabete gebraucht wurden und diese statt durch die ersten zehn Alphabetbuchstaben, durch die Ziffern 0 bis 9 bezeichnet werden. Kryptologisch liegen darin nur Nachteile.

LITERAE SCRIPTI.

LITERAE CLARIS.											
AB	a	b	c	d	e	f	g	h	i	l	m
	n	o	p	q	r	ſ	t	u	x	y	z
CD	a	b	c	d	e	f	g	h	i	l	m
	z	n	o	p	q	r	ſ	t	u	x	y
EF	a	b	c	d	e	f	g	h	i	l	m
	y	z	n	o	p	q	r	ſ	t	u	x
GH	a	b	c	d	e	f	g	h	i	l	m
	x	y	z	n	o	p	q	r	ſ	t	u
IL	a	b	c	d	e	f	g	h	i	l	m
	u	x	y	z	n	o	p	q	r	ſ	t
MN	a	b	c	d	e	f	g	h	i	l	m
	t	u	x	y	z	n	o	p	q	r	ſ
OP	a	b	c	d	e	f	g	h	i	l	m
	ſ	t	u	x	y	z	n	o	p	q	r
QR	a	b	c	d	e	f	g	h	i	l	m
	r	ſ	t	u	x	y	z	n	o	p	q
ST	a	b	c	d	e	f	g	h	i	l	m
	q	r	ſ	t	u	x	v	z	n	o	p
VX	a	b	c	d	e	f	g	h	i	l	m
	p	q	r	ſ	t	u	x	y	z	n	o
YZ	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	ſ	t	u	x	y	z	n

Abb. 53. Elf involutorische Alphabete für polyalphabetische Chiffrierung (*Porta* 1563)

7.4.5 Eine andere Familie von elf involutorischen Substitutionen benutzte schon 1563 *Giovanni Battista Porta* (Abb. 53). Man spricht hier von **verschobenen involutorischen Alphabeten**, die homophonisch durch 22 Schlüsselbuchstaben bezeichnet werden. Eine ähnliche Anordnung mit zehn Alphabeten ($V = Z_{20}$) wurde 1589 auch von den beiden *Argentis* benutzt (Abb. 69). Wir werden hier von PORTA-Chiffrierschritten sprechen.

[10] Von *Caspar Schott* in der *Schola steganographia* 1665 dem *Grafen Gronsfeld* zugeschrieben. Die GRONSFELD-Chiffrierung gebrauchte *Jules Verne* 1881 in der Erzählung *The Giant Raft.* 1892 wurde sie von französischen Anarchisten benutzt und von *Bazeries* gebrochen.

7.5 Unabhängige Alphabete

Porta brachte sich selbst um den Ruhm, Erfinder einer allgemeinen polyalphabetischen Substitution zu sein, die auf einer Anzahl θ ($\theta \leq (N^n)!$) von „gegenseitig unabhängigen“ permutierten Alphabeten beruht; das heißt von Alphabeten, die jedenfalls nicht durch so einfache Gesetzmäßigkeiten wie Verschiebung oder Rotation zusammenhängen. *Kahn* charakterisiert dies so: “*The order of the letters in the tableau may be arranged arbitrarily, provided no letter is omitted*”.

7.5.1 Obwohl *Porta* diesen Fall beschrieb, illustrierte er ihn nur mit verschobenen involutorischen Alphabeten wie in Abb. 53.[11] Es ist auch heute noch schwierig, in der Literatur Beispiele für den allgemeinen Fall nichtzyklischer Alphabete zu finden; *Smith, Gaines* behandeln ihn gar nicht, *Eyraud* diskutiert ihn wenigstens (‘*alphabets indépendants*’, speziell ‘*alphabets réellement non-parallèles*’, siehe 7.5.4). Wir werden in diesem ganz allgemeinen Fall von Permutationen kurz von PERMUTE-**Chiffrierschritten** sprechen.

Eine Tafel für allgemeine polyalphabetische Substitution könnte etwa lauten (man beachte den zu ihrer Konstruktion benutzten Kennsatz)

	a	d	f	g	j	k	m	p	q	s	t	u	v	w	x	y	z	h	e	i	n	r	c	b	o	l
A	**E**	**S**	**W**	**A**	**R**	B	C	D	F	G	H	I	J	K	L	M	N	O	P	Q	T	U	V	X	Y	Z
N	V	W	X	Y	Z	**S**	**C**	**H**	**O**	**N**	A	B	D	E	F	G	I	J	K	L	M	P	Q	R	T	U
S	P	Q	R	S	T	V	W	X	Y	Z	**D**	**U**	**N**	**K**	**E**	A	B	C	F	G	H	I	J	L	M	O
I	J	K	M	N	O	P	Q	R	T	U	V	W	X	Y	Z	**L**	**A**	**S**	**I**	**C**	B	D	E	F	G	H
C	C	D	E	F	G	J	K	L	M	P	Q	R	S	T	U	V	W	X	Y	Z	**H**	**I**	**N**	**B**	**O**	A
H	**A**	**K**	**M**	**I**	B	C	D	E	F	G	H	J	L	O	P	Q	R	S	T	U	V	W	X	Y	Z	**N**
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

7.5.2 Allgemeine polyalphabetische Substitution liegt vor im wenig bekannten Chiffriergerät von 1786 des schwedischen Freiherrn *Fredrik Gripenstierna* (1728–1804), für König *Gustav III.* von Schweden gebaut (Abb. 54). Das praktische Gerät besaß 57 Scheiben, jede für eine andere (feste) Substitution $Z_{26} \to Z_{10}^2$, vgl. 3.3.1. Durch Permutation der Scheiben konnte der Schlüssel verändert werden — im Prinzip gab es immerhin $57! \approx 4.05 \cdot 10^{76}$ Alphabete. Selbst wenn man das Alphabet nur nach, sagen wir, einigen hundert Zeichen wechselte, war diese Chiffrierung besser als alles zu dieser Zeit.

Gleichermaßen beschrieb in seiner ‚Geheimschreibkunst‘ von 1799 der Jesuitenpriester *Johann Baptist Andres* den Gebrauch einer Tafel mit 26 unabhängigen permutierten Alphabeten, die periodisch nach Maßgabe eines Schlüssels ausgewählt werden sollten.

---

[11] *Eyraud*, ehemals im kryptographischen Büro der Vichy-Regierung arbeitend, will diesen Ruhm, etwas chauvinistisch, allein dem Franzosen *Vigenère* zubilligen. Ähnlich versucht *Luigi Sacco*, Autor des vorzüglichen *Manuale di crittografia* (3. Aufl. Rom 1947), Italien zu begünstigen (*Kahn: trying to prove that everything was an Italian first*). *Charles J. Mendelsohn*, der über solcherlei Verdacht erhaben ist, preist *Porta* jedenfalls als “*the outstanding cryptographer of the Renaissance*”.

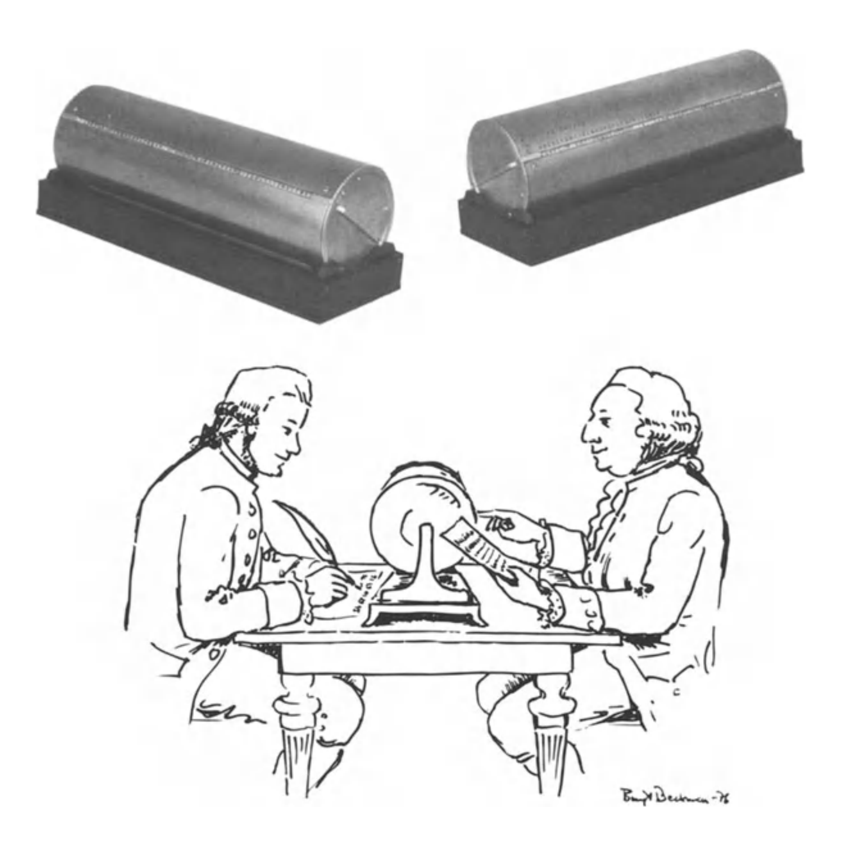


Abb. 54. Chiffriergerät des Freiherrn *Fredrik Gripenstierna*. Rekonstruktion durch Crypto AG, Zug. Unterlagen entdeckt durch *Sven Wäsström* im Staatsarchiv Stockholm

1915 baute der Schwede *Arvid Damm* eine Maschine, genannt A-21, bei der eine Anzahl austauschbarer Lineale mit unabhängigen permutierten Alphabeten auf einer Trommel parallel zur Achse angeordnet war (Abb. 55). Die Lineale befanden sich neben einem Lineal für das Klaralphabet, nach jeder Ablesung wurden sie um einen Schritt weitergeschoben. Das Lineal für das Klaralphabet konnte zwei Lagen einnehmen, diese wechselten mit einer relativ kurzen Periode. Diese Maschine war der von Gripenstierna weit unterlegen.

Polyalphabetische Chiffrierung mit unabhängigen permutierten Alphabeten wurde im 1. Weltkrieg von einer deutschen Funkstelle für Nachrichten an eine Sabotagegruppe in Nordafrika benutzt (,Für GOD'-System) und von der U.S. Air Force im 2. Weltkrieg für Boden-Luft-Verkehr (SYKO) verwendet — und jeweils von der gegnerischen Seite gebrochen. SYKO bestand aus dreißig involutorischen permutierten Alphabeten, die auf Karten gedruckt waren, die alte LARRABEE-Idee (7.4.1). Die Alphabete wurden zyklisch wiederholt benutzt, der Chiffrierer benutzte einen Indikator, um dem Dechiffrierer für einen vollen Tag den Beginn anzuzeigen. Dies war viel zu lang; die Schlüsselvereinbarung erlaubte den Einbruch in das andernfalls recht sichere System.

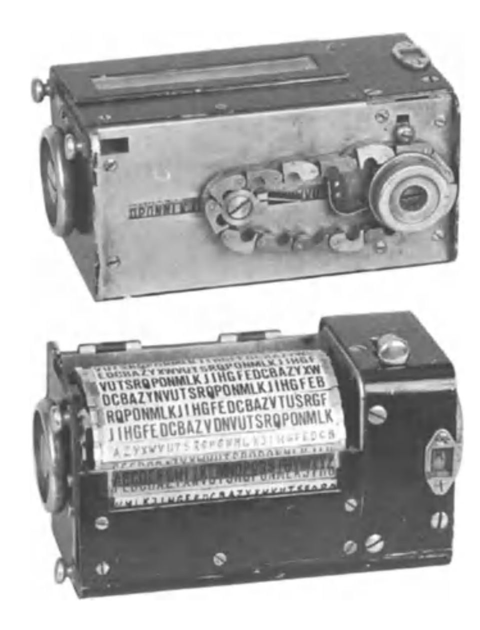
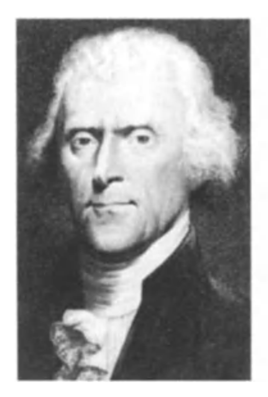


Abb. 55. A-21 von *Arvid Damm*

7.5.3 Unter Beschränkung auf voll zyklische Permutationen (‘*multiplex systems*’) hat polyalphabetische Chiffrierung mit „unabhängigen“ permutierten Alphabeten klassische Verwendung gefunden in Form spezieller Geräte, der Zylinder von *Jefferson* und *Bazeries*. Dabei werden die einzelnen voll zyklischen Substitutionen als Zyklen auf dem Rand einer Scheibe dargestellt. *Jefferson* ordnete (um 1795) 36 solcher dünner Scheiben (jede mit einem permutierten Z_{26}) zu einem langen Zylinder an; *Bazeries* (1891) verwendete 20 Scheiben (jede mit einem permutierten Z_{25}), wie in Abb. 19 gezeigt.





Thomas Jefferson



Parker Hitt



Joseph O. Mauborgne

Vierzehn von *Bazeries*’ Zyklen, die in Abb. 56 wiedergegeben sind, entsprangen launigen Einfällen, Merkversen wie

Allons enfants de la patrie, le jour de gloire est arrivé
Bienheureux les pauvres d'esprit, le royaume des Cieux
Charybde et Scilla
Dieu protège la France
Evitez les courants d'air
Formez les faisceaux
Gloire immortelle de nos aïeux
Honneur et Patrie
Instruisez la jeunesse
J'aime l'oignon frit à l'huile
Kyrie eleison
L'homme propose et Dieu dispose
Montez à cheval
Nous tenons la clef

1	a b c d e f g h i j k l m n o p q r s t u v x y z
2	b c d f g h j k l m n p q r s t v x z a e i o u y
3	a e b c d f g h i o j k l m n p u y q r s t v x z
4	z y x v u t s r q p o n m l k j i h g f e d c b a
5	y u z x v t s r o i q p n m l k e a j h g f d c b
6	z x v t s r q p n m l k j h g f d c b y u o i e a
7	a l o n s e f t d p r i j u g v b c h k m q x y z
8	b i e n h u r x l s p a v d t o y m c f g j k q z
9	c h a r y b d e t s l f g i j k m n o p q u v x z
10	d i e u p r o t g l a f n c b h j k m q s v x y z
11	e v i t z l s c o u r a n d b f g h j k m p q x y
12	f o r m e z l s a i c u x b d g h j k n p q t v y
13	g l o i r e m t d n s a u x b c f h j k p q v y z
14	h o n e u r t p a i b c d f g j k l m q s v x y z
15	i n s t r u e z l a j b c d f g h k m o p q v x y
16	j a i m e l o g n f r t h u b c d k p q s v x y z
17	k y r i e l s o n a b c d f g h j m p q t u v x z
18	l h o m e p r s t d i u a b c f g j k n q v x y z
19	m o n t e z a c h v l b d f g i j k p q r s u x y
20	n o u s t e l a c f b d g h i j k m p q r v x y z

Abb. 56. Die 20 Zyklen von *Bazeries*

Bazeries konnte den französischen Generalstab nicht dazu bewegen, seine Erfindung zu übernehmen – es gelang *de Viaris* (s. 14.3) zu zeigen, wie man mit dem Zylinder chiffrierte Nachrichten brechen kann, wenn man die Alphabete kennt, im militärischen Einsatz ein durchaus realistischer Fall (vgl. 2.1.2). Offenbar wußte *Bazeries* nicht, daß *Jefferson* lange vor ihm den selben Gedanken gehabt hatte, und wahrscheinlich erfuhr er auch nicht mehr – er starb 1931, 85 Jahre alt – daß 1922 die U.S. Army ihm, wie man sehen wird, eine späte Rechtfertigung gab. Auf den Zylindern von *Jefferson* und *Bazeries* brauchte man übrigens den chiffrierten Text nicht in der Zeile unterhalb des eingestellten Klartextes abzulesen – man konnte eine willkürlich gewählte i-te Zeile (die ‚i-te Generatrix') herausgreifen. Die Chiffrierung war demnach *polyphon*. Der Dechiffrierer suchte einfach, nachdem er den Geheimtext eingestellt hatte, nach einer Zeile, in der der Klartext „in die Augen sprang". Für

die unbefugte Entzifferung birgt diese Komplikation weniger Schwierigkeiten als man naiverweise erwarten möchte (s. 14.3.1).

Normalerweise blieb die Reihenfolge der Scheiben unverändert für eine ganze Nachricht, oder für eine vordefinierte Zeitspanne, etwa einen Tag.

Eine Ähnlichkeit mit dem Zylinder von *Bazeries* zeigt ein von dem italienischen Oberst *O. Ducros* 1901 vorgeschlagenes Gerät mit 13 Scheiben.

Anstatt mit Scheiben kann man mit Linealen (auf denen die Alphabete dupliziert sind) ebensogut arbeiten. Ein solches Gerät wurde schon 1893 von dem Franzosen *Arthur J. Hermann* vorgeschlagen. Eine Ausführung mit 25 Linealen ('*strips*') propagierte der damalige Hauptmann der U.S. Army, der spätere Oberst *Parker Hitt* 1914, auf *Bazeries* aufbauend. Er hatte zunächst keinen Erfolg. In der Zwischenzeit, 1917, erfand ein Marineleutnant, *Russell Willson*, ebenfalls ein Schiebergerät, das als NCB ('*Navy Code Box*') mindestens bis 1935 in Gebrauch war. Die U.S. Army aber wandte sich 1922 nach Verbesserungen von *Mauborgne* doch dem Zylinder zu. Das Gerät M-94 hatte 25 Aluminiumscheiben von Dollargröße auf einer 11 cm langen Spindel (Farbtafel D, Abb. 57); es wurde ab 1943 durch die dann verfügbare M-209 ersetzt.



Abb. 57. Zusammenbau der M-94.

1934 kam schließlich M-138-A, eine Schieberversion, in Gebrauch; von 100 verfügbaren Linealen wurden jeweils 30 benützt. M-138-A ('*strip cipher*') wurde im militärischen und im diplomatischen Dienst benutzt. Farbtafel E zeigt eine frühe Variante, M-138-T4. Man betrachtete das Schiebergerät als so sicher, daß man einen Funkspruch von *Roosevelt* an *Churchill*, unmittelbar nach der Atlantik-Konferenz, damit zu verschlüsseln wagte – sehr zum Mißvergnügen des mißtrauischen, weil kryptographisch erfahrenen *Roosevelt*. Anscheinend gelang es den Japanern nicht, die M-138-A zu brechen, wohl

aber den Deutschen. 1944 erzielte *Hans Rohrbach* den Einbruch (s. 14.3.3), und zwar ohne im Besitz der Alphabete zu sein. Zu diesem Zeitpunkt wechselten aber die U.S.A. u.a. zu den SIGTOT Vernam-Maschinen (s. 8.3.2).

Das von *Rohrbach* gebrochene System O-2 des U.S. State Department verwendete 30 von verfügbaren 50 Linealen, und zwar in zwei Gruppen von je 15 Linealen. Jedenfalls sollte die Anzahl der verfügbaren Scheiben oder Lineale deutlich größer sein als die Periode, d.h. die Anzahl der verwendeten.

Die U.S. Navy verwendete übrigens, als Nachfolger der *Code Box*, das Gerät CSP-642, ebenfalls mit 30 Linealen. Die Japaner erbeuteten einige dieser Schiebergeräte und mühten sich redlich damit ab – sie beachteten anscheinend die Methoden von *de Viaris* und *Friedman* nicht.

Für Zylinder- wie für Schiebergeräte bezeichnen wir, *Friedman* folgend, die einzelnen Chiffrierschritte als MULTIPLEX-**Chiffrierschritte**. Sie sind spezielle, nämlich voll zyklische PERMUTE-Chiffrierschritte.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z
1	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z	a
2	e	c	d	f	i	g	h	j	o	k	l	m	n	p	u	q	r	s	t	v	y	x	z	b	a
3	e	c	d	f	b	g	h	i	o	k	l	m	n	p	j	u	r	s	t	v	y	x	z	q	a
4	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y
5	j	y	b	c	a	d	f	g	q	h	e	k	l	m	i	n	p	o	r	s	z	t	v	u	x
6	z	y	b	c	a	d	f	g	e	h	j	k	l	m	i	n	p	q	r	s	o	t	v	u	x
7	l	c	h	p	f	t	v	k	j	u	m	o	q	s	n	r	x	i	e	d	g	b	y	z	a
8	v	i	f	t	n	g	j	u	e	k	q	s	c	h	y	a	z	x	p	o	r	d	l	m	b
9	r	d	h	e	t	g	i	a	j	k	m	f	n	o	p	q	u	y	l	s	v	x	z	b	c
10	f	h	b	i	u	n	l	j	e	k	m	a	q	c	t	r	s	o	v	g	p	x	y	z	d
11	n	f	o	b	v	g	h	j	t	k	m	s	p	d	u	q	x	a	c	z	r	i	y	e	l
12	i	d	u	g	z	o	h	j	c	k	n	s	e	p	r	q	t	m	a	v	x	y	b	f	l
13	u	c	f	n	m	h	l	j	r	k	p	o	t	s	i	q	v	e	a	d	x	y	b	z	g
14	i	c	d	f	u	g	j	o	b	k	l	m	q	e	n	a	s	t	v	p	r	x	y	z	h
15	j	c	d	f	z	g	h	k	n	b	m	a	o	s	p	q	v	u	t	r	e	x	y	i	l
16	i	c	d	k	l	r	n	u	m	a	p	o	e	f	g	q	s	t	v	h	b	x	y	z	j
17	b	c	d	f	l	g	h	j	e	m	y	s	p	a	n	q	t	i	o	u	v	x	z	r	k
18	b	c	f	i	p	g	j	o	u	k	n	h	e	q	m	r	v	s	t	d	a	x	y	z	l
19	c	d	h	f	z	g	i	v	j	k	p	b	o	t	n	q	r	s	u	e	x	l	y	m	a
20	c	d	f	g	l	b	h	i	j	k	m	a	p	o	u	q	r	v	t	e	s	x	y	z	n

Tabelle 2a. Die 20 permutierten Alphabete, die zu den Zyklen von *Bazeries* gehören.

7.5.4 Im Spezialfall $\theta \leq N$ kann man verlangen, daß N permutierten Alphabete von je N Zeichen, zeilenweise angeschrieben, die folgende Eigenschaft haben: In keiner Spalte kommt ein Zeichen mehr als einmal vor (*Eyraud*: '*alphabets réellement non-parallèles*'). Im Falle $\theta = N$ bilden dann die permutierten Alphabete ein ‚lateinisches Quadrat', d.h. daß auch in jeder Spalte jedes Zeichen genau einmal vorkommt. Solches hatte schon *Andres*[12]

[12] *Andres* begründete das allerdings noch damit, daß man die Tafel dann drehen konnte.

in seiner *Geheimschreibekunst*, 1799 vorgeschlagen. Die *'tabula recta'* erfüllt diese Vorschrift trivialerweise; sie trägt aber keine unabhängigen permutierten Alphabete.

Gleiches kann man von den permutierten Alphabeten fordern, die zu Zyklen (7.5.3) gehören; die Vorschrift verhindert dann den Angriff von *de Viaris* (s. 14.3.1). Die aus Merksätzen entstandenen Zyklen von *Bazeries* sind jedoch wenig geeignet; tatsächlich zeigen die zugehörigen permutierten Alphabete (Tabelle 2a) eigenartige Effekte: in den meisten Spalten treten ein oder zwei Buchstaben gehäuft auf. Es ist klar, daß das Fehlen vieler anderer Buchstaben eine Hilfe für eine unbefugte Entzifferung ist. Die zu den Zyklen von *Bazeries* gehörigen permutierten Alphabete können — ganz gleich wie man sie durch weitere fünf Zyklen ergänzt — kein lateinisches Quadrat ergeben.

Als Normalform für ein lateinisches Quadrat wählt man üblicherweise für die erste Zeile und für die erste Spalte, wie bei der *'tabula recta'*, ein Standardalphabet von N Zeichen. Dann gibt es für $N = 2$ und $N = 3$ nur die trivialen Lösungen einer *tabula recta*

a	b
b	a

a	b	c
b	c	a
c	a	b

Für $N = 4$ gibt es neben der *tabula recta* weitere drei solcher ‚reduzierten' lateinischen Quadrate:

a	b	c	d
b	c	d	a
c	d	a	b
d	a	b	c

a	b	c	d
b	d	a	c
c	a	d	b
d	c	b	a

a	b	c	d
b	a	d	c
c	d	a	b
d	c	b	a

a	b	c	d
b	a	d	c
c	d	b	a
d	c	a	b

Die Anzahlen wachsen rasch, für $N{=}5$ sind es 56, für $N{=}6$ sind es 9408, für $N{=}7$ bereits 16 942 080, für $N{=}8$ schon 535 281 401 856. Für $N{=}9$ hat man bereits $\approx 3.78 \cdot 10^{17}$ (*Bammel, Rothstein* 1975), während die Gesamtanzahl aller reduzierten Sätze von 9 Alphabeten mit 9 Zeichen $(8!)^8 \approx 6.98 \cdot 10^{36}$ beträgt.

Nachfolgend zwei lateinische Quadrate für $N = 10$ mit $Z_{10} = \{0, 1, 2, \ldots, 9\}$:

0	1	2	3	4	5	6	7	8	9
1	5	7	2	8	9	0	3	4	6
2	4	6	1	3	8	9	0	5	7
3	0	5	7	2	4	8	9	6	1
4	9	0	6	1	3	5	8	7	2
5	8	9	0	7	2	4	6	1	3
6	7	8	9	0	1	3	5	2	4
7	6	1	8	9	0	2	4	3	5
8	3	4	5	6	7	1	2	9	0
9	2	3	4	5	6	7	1	0	8

0	1	2	3	4	5	6	7	8	9
1	4	3	2	0	9	8	5	6	7
2	6	5	4	3	0	9	8	7	1
3	8	7	6	5	4	0	9	1	2
4	9	8	1	7	6	5	0	2	3
5	0	9	8	2	1	7	6	3	4
6	7	0	9	8	3	2	1	4	5
7	2	1	0	9	8	4	3	5	6
8	3	4	5	6	7	1	2	9	0
9	5	6	7	1	2	3	4	0	8

Tabelle 2b zeigt das Standardalphabet und die Alphabete, die zu den 25 Zyklen der M-94 gehören; sie bilden mit drei Ausnahmen ein lateinisches Quadrat. Warum *Mauborgne* diese Ausnahmen vorsah, ist nicht bekannt.

Beachte auch, daß die rotierten Alphabete (7.2.2) — anders als die verschobenen Alphabete (7.2.1) — gewöhnlich kein lateinisches Quadrat bilden.

Einfache Formeln für die Anzahl $l(N)$ reduzierter lateinischer Quadrate von N Zeilen und N Spalten wurden bisher nicht angegeben. *Erdős* (1913–1996) und *Kaplanski* vermuteten 1946, daß asymptotisch gilt

$$l(N) \asymp N \cdot (N!)^{N-2}/e^{N\cdot(N-1)/2} \qquad (l(9) < 1.73 \cdot 10^{24}).$$

Für $N \leq 9$ ist eine bessere obere Schranke

$$l(N) \leq \sqrt{((N-1)!)^{N-1}} \qquad (l(9) < 2.64 \cdot 10^{18}).$$

Eine sehr grobe untere Schranke ist (*Werner Heise*)

$$l(N) \geq 2! \cdot 3! \cdot 4! \cdot \ldots \cdot (N-2)! \qquad (l(9) > 1.25 \cdot 10^{11}).$$

Beachte, daß $l(9) = 3.78 \cdot 10^{17}$. Für $l(26)$ geben die angegebenen Schranken $10^{243} < l(26) < 10^{498}$. Man darf etwas wie $l(26) \approx 10^{320}$ erwarten.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	b	c	e	j	i	v	d	t	g	f	z	r	h	a	l	w	k	x	p	q	y	u	n	s	m	o
2	c	a	d	e	h	i	z	f	j	k	t	m	o	p	u	q	x	w	b	l	v	y	s	r	g	n
3	d	g	z	k	p	y	e	s	n	u	o	a	j	x	m	h	r	t	c	v	b	w	l	f	q	t
4	e	i	b	c	d	g	j	l	f	h	m	k	r	w	q	t	v	u	a	n	o	p	y	z	x	s
5	f	r	y	o	m	n	a	c	t	b	d	w	z	q	p	i	u	h	l	j	k	x	e	g	s	v
6	g	j	i	y	t	k	p	w	x	s	v	u	e	d	c	o	f	n	q	a	r	m	b	l	z	h
7	h	n	f	u	z	m	s	x	k	e	p	c	q	i	g	v	t	o	y	w	l	r	a	j	d	b
8	i	w	v	x	r	z	t	p	h	o	c	q	g	s	b	j	e	y	u	d	m	f	k	a	n	l
9	j	x	r	s	f	h	y	g	v	d	q	p	b	l	i	m	o	a	k	z	n	t	c	w	u	e
10	k	d	a	f	l	j	h	o	c	g	e	b	t	m	n	r	s	q	v	p	x	z	i	y	w	u
11	l	e	g	i	j	b	k	u	z	a	r	t	s	o	h	n	p	f	x	m	w	q	d	v	c	y
12	m	y	u	v	w	l	c	q	s	t	x	h	n	f	a	z	g	d	r	b	j	e	o	i	p	k
13	n	m	j	h	a	e	x	b	l	i	g	d	k	c	r	f	y	p	w	s	z	o	q	u	v	t
14	o	l	t	w	g	a	n	z	u	v	j	e	f	y	d	k	h	s	m	x	q	i	p	b	r	c
15	p	v	x	r	n	q	u	i	y	z	s	j	a	t	w	b	d	l	g	c	e	h	f	o	k	m
16	q	t	s	**e**	o	p	i	d	m	n	f	x	w	u	k	y	j	v	h	g	**b**	l	z	c	**a**	r
17	r	k	w	p	u	t	q	e	b	x	l	n	y	v	f	c	i	m	z	h	s	a	g	d	o	j
18	s	o	n	m	q	u	v	a	w	r	y	g	c	e	z	l	b	k	d	f	i	j	x	h	t	p
19	t	s	m	z	k	x	w	v	r	y	u	f	i	g	j	d	a	b	e	o	p	c	h	n	l	q
20	u	p	k	g	s	c	f	j	o	w	a	y	d	h	v	e	l	z	n	r	t	b	m	q	i	x
21	v	f	l	q	y	s	o	r	p	m	h	z	u	k	x	a	c	g	j	i	d	n	t	e	b	w
22	w	h	o	l	b	d	m	k	e	q	n	i	x	r	t	u	z	j	f	y	c	s	v	p	a	g
23	x	z	p	t	v	o	b	m	q	c	w	s	l	j	y	g	n	e	i	u	f	d	r	k	h	a
24	y	q	h	a	c	r	l	n	d	p	b	o	v	z	s	x	w	i	t	e	g	k	u	m	j	f
25	z	u	q	n	x	w	r	y	a	l	i	v	p	b	e	s	m	c	o	k	h	g	j	t	f	d

Tabelle 2b. ‚Fast' lateinisches Quadrat, das zu *Mauborgne*s Alphabeten der M-94 gehört. Eine zyklische Permutation der drei fettgedruckten Buchstaben in der Zeile 16 ergibt ein korrektes lateinisches Quadrat.

8 Polyalphabetische Chiffrierung: Schlüssel

"No message is safe in cipher unless the key phrase is comparable in length with the message itself."
Parker Hitt, 1914

8.1 Frühe Verfahren mit periodischen Schlüsseln

8.1.1 Die frühesten Ansätze zu einer polyalphabetischen Chiffrierung finden sich bei *Leon Battista Alberti* (1404–1472) in einem Werk von 1466, einem Essay von 25 Seiten, das er für *Dato*, den Päpstlichen Sekretär, schrieb.[1] Aufbauend auf seinen Überlegungen zur Kryptanalyse erkannte *Alberti*, daß es beim Gebrauch einer einfachen Substitution nicht ausreichte, sie von Zeit zu Zeit zu wechseln. So schlug er vor, nach jeweils drei oder vier Wörtern zu einem anderen Alphabet überzugehen, und erfand die drehbare Scheibe (Abb. 26), um mehrere begleitende Alphabete verfügbar zu haben. Drei oder vier Wörter – das sind durchschnittlich 18 Buchstaben: damit blieb *Alberti* unbewußt unter der *Shannon*schen Unizitätslänge für die einfache Substitution. Gegenüber der damals schon geläufigen Verwendung von Homophonen war ein großer Fortschritt erzielt: Bedeutete bei einer einfachen Substitution $Z_{25} \dashrightarrow Z_{10}^2$ vielleicht 89 , 43 , 57 und 64 den Buchstaben /a/, so konnte jetzt jedes Bigramm /a/ bedeuten.

Die Ziffern in *Alberti*s Scheibe dienten übrigens (auch) der polyalphabetischen Chiffrierung von Codes, und zwar eines Codes von 336 Zweier-, Dreier- und Vierergruppen, gebildet aus den Ziffern /1/ , /2/ , /3/ , /4/ ; die Codegruppen waren in den Text einzustreuen.[2]

---

[1] Das lateinische Original "De cifris" ist abgedruckt in *Aloys Meister*, ‚Die Geheimschrift im Dienste der Päpstlichen Kurie', Paderborn, Schöningh, 1906, S. 125–141. Italienische Übersetzung "Trattati in cifra", Rom um 1470 .

[2] Über die Art und Weise, wie mit *Alberti*s Scheibe der Wechsel des Alphabets bestimmt werden sollte, ist sich die Sekundärliteratur nicht ganz klar. *Sacco* (∗ 1884), ein italienischer, und *Eyraud* († 1963), ein französischer Kryptologe, deuten es so: Der Chiffrierer setzt vor jedes Teilstück, das mit einer neuen Stellung der Scheibe chiffriert werden soll, eine der Ziffern /1/ bis /4/ . Die jeweilige Anfangsstellung der (bei Chiffrierer und Dechiffrierer identischen) Scheibe ist dadurch fixiert, daß der Indikator (frz. *index*), ein vereinbartes Klartextzeichen — sagen wir /b/ — mit dem wählbaren ersten Geheimtextzeichen zur Deckung gebracht wird. Jedes neue Teilstück wird durch Übertragung der chiffrierten Ziffer angekündigt, anschließend stellt auch der Dechiffrierer das nächste übertragene Geheimtextzeichen dem Index gegenüber. Um dieses

Alberti sprach auch schon davon, den Code für das Chiffrieren nach Wörtern und für das Dechiffrieren nach Gruppen zu ordnen. Ob dieser frühe zweiteilige Code den Zweck erhöhter Sicherheit hatte, kann nicht eindeutig festgestellt werden.

Alberti jedenfalls darf mit diesen Leistungen als „Vater der modernen Kryptologie“ bezeichnet werden, obschon die Leistungen des Renaissancearchitekten – der Palazzo Pitti, Sant' Andrea in Mantua, Santa Maria Novella in Florenz, der Tempio Malatestiana zu Rimini – nicht zurückstehen müssen.

8.1.2 War *Alberti* nach jeweils „drei oder vier“ Wörtern zu einem anderen Alphabet übergegangen, so schlug *Trithemius* 1518 bereits vor, nach jedem Buchstaben zum nächsten Alphabet überzugehen, und so nach einer festen Progressionsvorschrift, nämlich Zeile für Zeile, alle verfügbaren Alphabete zu benützen, bevor ein Alphabet zum zweiten Male benutzt wird.[3] Aber das ist ein festes Verfahren mit einer Periode 24, das *Alberti* weit unterlegen war. Man sollte meinen, daß dies im 20. Jahrhundert nur noch historisch interessant gewesen wäre, aber tatsächlich wurde ein solches Verfahren mit einer Periode 3, gefolgt von Spaltentransposition, von den Franzosen *A B C* genannt, 1914 an der Westfront eingesetzt (vgl. 2.1.1).

Trithemius gab auch die erste Chiffriertafel (‘*tabula recta*’) an (Abb. 52). *Porta* zeigte dann 1602, wie man eine der Vorschrift von *Trithemius* folgende Chiffrierung – in heutiger Redeweise ein VIGENERE mit dem speziellen Schlüssel $A\ B\ C\ \dots\ Y\ Z$ – angreifen kann: Wenn im Klartext drei konsekutive Buchstaben sind, wie *pon* in *pondus*, ergibt sich im Geheimtext ein Buchstabentripel.

Das Verdienst, die Chiffrierung durch Angabe eines **Schlüsselworts** zur Bestimmung der sukzessiven Verdrehung der Scheibe oder zur Auswahl der Zeile der Tafel erweitert zu haben, kommt *Giovanni Battista Belaso* (1553) zu. Er benutzte auch bereits ziemlich lange Schlüsselworte, (die notfalls periodisch wiederholt wurden) wie *OPTARE MELIORA* und *VIRTUTI OMNIA PARENT*. Es handelt sich hier um einen **periodischen**, d.h. endlichen, periodisch wiederholten Schlüssel, der eine periodische polyalphabetische Chiffrierung (2.3.3) ergibt. Aber *Trithemius* wie auch *Belaso* verwendeten nur das Standardalphabet – im Gegensatz zu *Alberti*, der ein beliebiges gemischtes Alphabet P zuließ, um daraus durch *Verschiebung* andere herzuleiten.

Die kombinatorische Komplexität Z des Verfahrens mit einem Standardalphabet von N Zeichen und einer Chiffrierbreite n ist, wenn das Schlüsselwort d Buchstaben hat, lediglich $(N^n)^d$, also hat man $Z = N^{n \cdot d}$.

Verfahren durchführen zu können, bräuchte man nicht unbedingt vier Ziffern /1/ bis /4/. Übrigens wäre dies das erste Vorkommen einer Schlüsselvereinbarung durch einen gedeckten Indikator, wie sie für moderne Schlüsselmaschinen geläufig ist.

[3] *Kahn* nennt das ‘progressive key’, s. 8.4.2 – nicht mit dem von *Friedman* benutzten Ausdruck ‘running key’ (‚fortlaufende Chiffrierung‘, 2.3.6) zu verwechseln. Moderne Chiffriermaschinen, die mit Vorliebe mit progressiver Chiffrierung arbeiten, verwenden allerdings weit mehr als zwei Dutzend Alphabete.

8.2 „Doppelter Schlüssel“

8.2.1 *Porta* (1535–1615) verband nun 1563 *Alberti*s Gebrauch eines permutierten Alphabets P mit *Belaso*s Gebrauch eines Schlüssels zur Bestimmung der Verdrehungen der Scheibe. Da auch ein Kennwort zur Festlegung des permutierten Alphabets als (wechselnder) Schlüssel dienen kann, sprach man von ‚doppelter Chiffrierung‘ (engl. *double cipher*), in der französischen Terminologie hat sich dies bis heute unter der Benennung *substitution à double clef* erhalten.[4] Das Kennwort wird manchmal auch ‚zweiter Schlüssel‘ genannt.

Die kombinatorische Komplexität Z des Verfahrens erhöht sich nun auf $(N^n)\,!\cdot(N^n)^{d-1}$, wenn ein beliebiges permutiertes Alphabet erlaubt wird und das Schlüsselwort d Buchstaben hat, also hat man $Z = (N^n - 1)\,!\cdot N^{n\cdot d}$.

Statt der Scheibe *Alberti*s kann natürlich auch eine Tafel benutzt werden. Diese würde für den Fall von Abb. 26 lauten (mit $\{\ \rho^{-i}P : i \in \mathbb{N}\ \}$)

	a	b	c	d	e	f	g	i	l	m	n	o	p	q	r	s	t	v	x	z	1	2	3	4
0	D	L	G	A	Z	E	N	B	O	S	F	C	H	T	Y	Q	I	X	K	V	P	&	M	R
1	R	D	L	G	A	Z	E	N	B	O	S	F	C	H	T	Y	Q	I	X	K	V	P	&	M
2	M	R	D	L	G	A	Z	E	N	B	O	S	F	C	H	T	Y	Q	I	X	K	V	P	&
3	&	M	R	D	L	G	A	Z	E	N	B	O	S	F	C	H	T	Y	Q	I	X	K	V	P
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Man erhält übrigens den Dechiffrierschritt, wenn man über eine *tabula recta* der Klartextzeichen das Geheimtextzeichenalphabet setzt, in unserem Beispiel (mit $\{\ P^{-1}\rho^{i} : i \in \mathbb{N}\ \}$)

	D	L	G	A	Z	E	N	B	O	S	F	C	H	T	Y	Q	I	X	K	V	P	&	M	R
0	a	b	c	d	e	f	g	i	l	m	n	o	p	q	r	s	t	v	x	z	1	2	3	4
1	b	c	d	e	f	g	i	l	m	n	o	p	q	r	s	t	v	x	z	1	2	3	4	a
2	c	d	e	f	g	i	l	m	n	o	p	q	r	s	t	v	x	z	1	2	3	4	a	b
3	d	e	f	g	i	l	m	n	o	p	q	r	s	t	v	x	z	1	2	3	4	a	b	c
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

8.2.2 Diese Verbindung der *tabula recta* mit einer beliebigen Substitution (vgl. 7.4.1) schlug 1585 *Vigenère* vor. Er erkannte auch, daß es wichtig war, möglichst lange Schlüsselwörter zu wählen, um die unbefugte Entzifferung zu erschweren.

Blaise de Vigenère wurde am 5. April 1523 in Saint-Pourçain geboren, “halfway between Paris and Marseilles”, schreibt in amerikanischer Großzügigkeit *Kahn*. Er studierte, und ging bei verschiedenen Herren in diplomatischen Dienst. Er las *Trithemius*, *Belaso*, *Cardano* und *Porta* und bekam Zugang zu *Alberti*s Manuskript. 1570 gab er seine Beschäftigungen auf und verlegte sich, 47 Jahre alt, ganz aufs Schreiben, schrieb bis zu seinem Tod 1596 über

[4] *Kahn* schreibt “Givierge was even then [1920] calling polyalphabetic systems by the almost obfuscatory *‘double substitution’* which tells absolutely nothing at all about the system.” *Givierge* sprach von *clef principale* für den eigentlichen Schlüssel.

alles Mögliche, auch einen *Traicté des Comètes.* Sein *Traicté des Chiffres* entstand 1585, "despite the distraction of a year-old baby daughter" (so schreibt *Kahn*) – *Vigenère* hatte 1570 die wesentlich jüngere *Marie Varé* geheiratet. Das Buch von über 600 Seiten enthielt vieles außer Kryptographie – japanische Ideogramme, Alchemie, Magie, Kabbala, Goldmacherrezepte, aber auch eine zuverlässige, genaue Wiedergabe des Standes der Kryptologie zu seiner Zeit. Bei der Diskussion polyalphabetischer Chiffrierung verwandte er wie *Alberti* und *Trithemius* durch Verschiebung eines Alphabets auseinander hervorgehende Alphabete, bezeichnete die Zeilen aber durch Schlüsselbuchstaben – wie schon *Belaso* und *Porta*, die allerdings involutorische Alphabete benutzt hatten.

8.2.3 Eine ‚dreifache Chiffrierung' (‘*treble key*’,‘*triple clef*’) bekommt man, wenn man *zwei* Substitutionen P_1, P_2 vorgibt und den Fall b) in 7.1.1 benützt, also die Menge von Alphabeten $\{ P_1 \rho^i P_2 : i \in \mathbb{N} \}$; siehe auch 19.5.3 . *Vigenère* gelangte zu diesem Fall, als er die VIGENÈRE-Chiffrierschritte mit einem *permutierten* Alphabet von Schlüsselbuchstaben bezeichnete.

8.3 Vernam-Chiffrierung

Moderne Nachrichtenverbindungen arbeiten in einem binären Alphabet $Z_2 \hat{=} \mathbb{Z}_2$. Will man die Zeichen des internationalen Fernschreibalphabets CCIT 2 chiffrieren, so kann man dies als eine polygraphische binäre Chiffrierung mit $N = 2$ und $n = 5$ auffassen. Für die Chiffrierung von Bytes, d.h. 8-Bit-Zeichen, die in heutigen Rechnern häufig als grundlegende Einheit dienen, handelt es sich um den Fall $N = 2$ und $n = 8$ der binären Oktogramme, für Blöcke von 8 Bytes um $N = 2$ und $n = 64$.

Beschränkt man sich auf VIGENÈRE-Chiffrierschritte, so gibt es deren 32 für $\mathbb{Z}_2^5$ bzw. 256 für $\mathbb{Z}_2^8$, ihre Durchführung als Addition *mod.* 32 bzw. 256 erfordert einen zyklischen Addierer mit 5 Bit bzw. 8 Bit Breite. Eine geeignete binäre Schaltung (mit $n = 5$) zeigt Abb. 58. Größere Mikroprozessoren erlauben heute sogar Verarbeitungsbreiten von 64 Bit und können damit Byte-Oktogramme direkt chiffrieren.

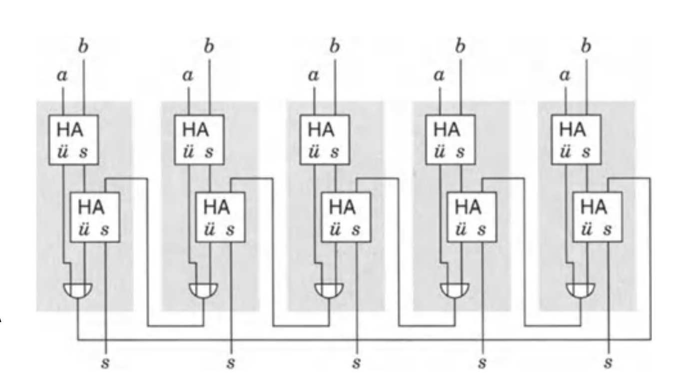


Abb. 58
Aus Halbaddierern **HA** aufgebautes 5-stelliges Additionsschaltnetz

8.3.1 Andererseits kann auch bitweise ein VIGENÈRE-Schritt vorgenommen werden. Dieser Extremfall der **bitweisen Binärchiffrierung** wird sich später als besonders wichtig erweisen. Ist eine Chiffrierung $\mathbb{Z}_2 \dashrightarrow \mathbb{Z}_2$ definal, so ist sie eine Permutation der beiden Elemente **O** und **L** , es gibt nur

die **Identität** $O : \begin{matrix} \mathbf{O} & \mapsto & \mathbf{O} \\ \mathbf{L} & \mapsto & \mathbf{L} \end{matrix}$ und die **Spiegelung** $L : \begin{matrix} \mathbf{O} & \mapsto & \mathbf{L} \\ \mathbf{L} & \mapsto & \mathbf{O} \end{matrix}$

als Chiffrierschritte (VERNAM-**Chiffrierschritte**). Die Chiffrierung ist notwendigerweise involutorisch, aber nicht echt involutorisch. Es ist $|M| = 2$, der kleinste Wert, der eine polyalphabetische Chiffrierung erlaubt. Als Schlüssel dient eine endliche (**O**,**L**)-Folge, die periodisch wiederholt wird, oder eine unendliche (**O**,**L**)-Folge.

In $\mathbb{Z}_2$ kann die Identität O durch $+\mathbf{O}$, die Addition von **O**, und die Spiegelung L durch $+\mathbf{L}$, die Addition von **L**, bewerkstelligt werden. Die Chiffrierung $\mathbb{Z}_2 \to \mathbb{Z}_2$ ist also eine lineare Transformation. Die Addition in $\mathbb{Z}_2$, die Addition *modulo* 2, oft mit $\oplus$ bezeichnet, fällt mit der Booleschen Operation $\not\leftrightarrow$ (**Bisubtraktion**, auch Antivalenz oder exklusives Oder (engl. *exclusive-Or, non-carry binary addition*) genannt, zusammen. Ihr Ergebnis fällt gerade am Summen-Ausgang eines Halbaddierers an.

8.3.2 Eine maschinelle Realisierung dieser beiden Schritte liegt nahe. Diese Idee hatte 1917 (also vor *Lester S. Hill*) ein junger Angestellter von AT & T in New York, *Gilbert S. Vernam* (1890–1960).

Vernam baute für einen Fernschreiber einen binären VIGENÈRE-Chiffrierzusatz. Der Schlüssel war auf Lochstreifen gestanzt und konnte zu einer ziemlich langen Schleife geklebt werden. Durch doppelte Chiffrierung mit Schleifen von 999 und 1000 Zeichen erzielte *Vernams* Mitarbeiter *Lyman F. Morehouse* einen Schlüssel, der 999000 Zeichen lang und, wichtiger, ‚sinnlos' war.

Gilbert S. Vernam reichte am 13. Sept. 1918 darauf ein US Patent ein und erhielt es 1919 unter der Nummer 1,310,719. Im kommerziellen Verkehr wurde es allerdings kein Erfolg, Codes waren beliebter. Die Idee wurde aber anderswo in der Fernschreibtechnik aufgegriffen, insbesondere im Siemens Doppel-Abtaster mit „Mischer" und in der SIGTOT-Maschine der U.S. Army.

8.3.3 Geht man von einem VIGENÈRE-Chiffrierschritt in $\mathbb{Z}_{2^n}$, bewirkt durch Addition von $(a_1\ a_2\ a_3\ \dots\ a_n)$ im Dualsystem, polyalphabetisch zu n VERNAM-Chiffrierschritten, also VIGENÈRE-Chiffrierschritten in $\mathbb{Z}_2$ mit der Addition von a_1 , von a_2 , ... , von a_n über, so entfällt gerade die Übertragseinrichtung des binären Additionsschaltnetzes. Entsprechendes gilt für VIGENÈRE-Schritte in $\mathbb{Z}_{10^n}$, die durch Addition *modulo* 10^n der Zahlen $\{0,\ 1,\ 2,\ \dots\ 10^n - 1\}$ auf einer n-stelligen mechanischen Tischrechenmaschine bewerkstelligt werden können. Geht man polyalphabetisch zu n VIGENÈRE-Schritten in $\mathbb{Z}_{10}$ über, so braucht man (vgl. 5.7) die Übertragseinrichtung nicht; eine solcherart verstümmelte Tischrechenmaschine erlaubt polyalphabetische Chiffrierung über ihre ganze Arbeitsbreite.

8.4 Quasi-nichtperiodische Schlüssel

8.4.1 Periodische polyalphabetische Chiffrierung hatte es trotz der Sicherheit, die sie bei sorgfältigem Gebrauch bot, schwer, sich gegen die Nomenklatoren durchzusetzen. Diese Chiffrierung wurde zunächst meist nur in Ausnahmefällen eingesetzt: In der Päpstlichen Kurie 1590, wo sie durch *Chorrin*, einen Entzifferer von *Henri* IV. gebrochen wurde; von den Aufständischen der Fronde 1654 im Briefwechsel zwischen dem Kardinal *de Retz* und dem Prinzen *Condé*, dem späteren *Louis* II. von Bourbon, gebrochen durch *Guy Joly*, der das Schlüsselwort erriet. So wendete auch *Marie Antoinette* sie (vgl. 2.1.1) in ihrem amourösen Schriftwechsel 1791 an. Ihr Geliebter seit 1783, der schwedische *Graf Axel Fersen*, erstellte eine Porta-ähnliche Anordnung mit 23 unabhängigen involutorischen Alphabeten (Abb. 59). *Axel Fersen* war vorsichtig, er benutzte keine naheliegenden Kennworte, sondern Wörter wie *DEPUIS, VOTRE*. Daß die Flucht *Ludwig* XVI. und *Maries* an der Brücke von Varenne entdeckt wurde, war nicht Schuld der Kryptographie: Keine ihrer beider Botschaften war entziffert worden.

A	(ab)	(cd)	(ef)	(gh)	(ik)	(lm)	(no)	(pq)	(rs)	(tu)	(xy)	(z&)
B	(bk)	(du)	(ei)	(fl)	(gn)	(ho)	(my)	(ps)	(qx)	(rt)	(ac)	(&z)
C	(lr)	(ad)	(bg)	(cz)	(s&)	(ek)	(fm)	(th)	(ix)	(np)	(oq)	(uy)
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Abb. 59. Marie Antoinette's polyalphabetische Chiffrierung.

Polyalphabetische Substitution hatte, bevor man sie mechanisierte, immer den Ruf, mühsam und fehleranfällig zu sein. 1819 schreibt *William Blair* in einem Enzyklopädieartikel *“polyalphabetic substitution requires too much time and by the least mistake in writing is so confounded ...”* .

Letzteres findet sich auch in einem Brüsseler Werk des 17. Jahrhunderts, *Traitté de l'art de deschiffrer*: *“... takes too long to encipher them, dropping of a single ciphertext letter garbles the message from that point on ...” (Kahn).*

8.4.2 Polyalphabetische Substitution galt aber auch als unbrechbar. *Matteo Argenti* schrieb, sie „ist die edelste und größte in der Welt, die sicherste und getreueste, so daß es niemals einem Menschen gelingt, sie zu brechen“.

Bis ins 19. Jahrhundert gelang ein echter Einbruch nur, wenn Standardalphabete (oder revertierte Standardalphabete) mit Verschiebung verwendet, Wörter aus dem Klartext erraten und der (zu kurze) Schlüssel rekonstruiert werden konnte, oder wenn gar, wie von *Porta* oder den *Argentis*, der Schlüssel erraten wurde. Mit der im 19. Jahrhundert aufkommenden systematischen Lösung der periodischen polyalphabetischen Chiffrierung ändert sich das.

Will man diese Angriffsmöglichkeit ausschließen, so muß man, *Parker Hitt* folgend, zu einer Periodenlänge greifen, die deutlich größer ist als die gesamte Nachricht (‚quasi-nichtperiodischer Schlüssel‘), oder man muß zu fortlaufenden Schlüsseln übergehen.

8.4.3 Wenn schon quasi-nichtperiodische Chiffrierung, dann sollten sicherheitshalber weit mehr Alphabete verwendet werden als man üblicherweise Schlüsselbuchstaben hat. Diese sollten zudem unregelmäßig ausgewählt werden (*Kahn*: '*irregular sequence of alphabets*'). Überdies liegt es bei so vielen Alphabeten nahe, progressive Chiffrierung im folgenden Sinne zu verwenden:

Die **progressive Chiffrierung** ist eine polyalphabetische Chiffrierung, bei der kein Alphabet wieder benutzt wird, bevor jedes andere Alphabet benutzt wurde. Eine progressive Chiffrierung ist also periodisch mit einer Periode gleich der Kardinalität θ der Menge der Chiffrierschritte; eine quasi-nichtperiodische Chiffrierung entsteht, wenn die Nachricht kürzer ist als θ .

Progressive Chiffrierung hatte schon *Trithemius* mit seiner '*tabula recta*' vorgeschlagen (7.3.1, 8.1.2). Progressive Chiffrierung ist systembedingt bei den Zylinder- und Streifengeräten, bei denen jedes Alphabet nur in *einer* Ausfertigung verfügbar ist. Progressive Chiffrierung verwendete man auch gern in den mechanischen oder elektronischen Chiffriermaschinen der ersten Hälfte des 20. Jahrhunderts.

8.4.4 Obwohl im Prinzip Rotoren viele Kontakte haben konnten (der Halbrotor der japanischen *angō kikai taipu A*, Abb. 66, hatte deren 60), schien es doch für ein Alphabet Z_N natürlich zu sein, Rotoren mit genau N Kontakten u versehen und damit genau $\theta = N$ Alphabete zu haben. Um hohe Werte von θ für eine progressive Chiffrierung zu erzielen, fanden *Hebern* und *Scherbius* unabhängig die Lösung, mehrere hintereinandergesetzte Rotoren wie bei einem Zähler zu schalten (**reguläre Rotor-Fortschaltung**), ein elementares Beispiel einer progressiven Chiffrierung. Für vier Rotoren und $\theta = 26^4$, wie in der ENIGMA, ist die Periode d gleich oder (bei ‚fast progressiver Chiffrierung') nur wenig kleiner als $\theta = 26^4 = 456\,976$. Das ist eine eindrucksvolle Anzahl, sie bedeutet, daß die Periode nicht ausgeschöpft werden muß für eine Nachricht von der Länge eines Romans. Für fünf Rotoren und $\theta = 26^5$ beträgt die Periode knapp 12 Millionen, das ist mehr als die ganze Bibel Buchstaben hat. Andrerseits ist es wenig im Vergleich zu den Möglichkeiten heutiger Nachrichtensysteme: Bereits Systeme mit einer Bitrate von 2 MBit/sec übertragen 12 Millionen Buchstaben in 48 Sekunden.

8.5 Maschinen mit eingebauten Schlüsselerzeugern

Moderne Chiffriermaschinen mit einigem Komfort haben eine doppelte Funktion: Sie vollziehen nicht nur polyalphabetische Chiffrierschritte, sie erzeugen auch ihre eigene Schlüsselzeichenfolge für die Auswahl dieser Chiffrierschritte. Die Schlüsselerzeugung ist die *crux* der kompletten Mechanisierung.

8.5.1 Bei *Trithemius* wurden die verschobenen (Standard-)Alphabete schlicht der Reihe nach verwendet. So geschah es noch im '*Cryptograph*' von *Wheatstone*, 1867 (Farbtafel C). Das lief auf den Gebrauch eines festen Schlüssels hinaus. Der Gebrauch von Schlüsseln durch *Belaso* (8.1.2) bedeutete bereits eine „Unregelmäßigkeit in der Auswahl der Alphabete“.

8.5.2 Schlüsselerzeuger, die so lange Perioden aufweisen, daß normalerweise für *eine* Nachricht die volle Periode bei weitem nicht ausgeschöpft wird, können durch die Wahl des Startpunktes in der Schlüsselzeichenfolge eine weitere, vom Chiffrierer herrührende „Unregelmäßigkeit“ einführen.

Arthur Scherbius, einer der Erfinder des Rotorprinzips, beschrieb in seiner grundlegenden Patentanmeldung vom 23. Februar 1918, DRP 416 219) zunächst nur vage als *eine* Möglichkeit die regelmäßige Rotor-Fortschaltung „wie bei Zählwerken“ durch Mitnehmer, d.h. eine reguläre Rotor-Fortschaltung.

Arvid Gerhard Damm, ein anderer Erfinder des Rotorprinzips, benutzt aber in seiner schwedischen Patentanmeldung vom 10. Oktober 1919 sogar einen Schlüsselerzeuger: vier ‚Antriebsräder‘, um die vier Halbrotoren nach jedem Chiffrierschritt eine unregelmäßige Anzahl von Positionen fortzuschalten. Die Periode betrug $17 \cdot 19 \cdot 21 \cdot 23$, also mehr als 150 000, somit etwa ein Drittel von $\theta = 26^4 = 456\,976$. Das war nahezu progressive Chiffrierung.

Scherbius nutzt dann in einer weiteren Anmeldung vom 26. September 1920 (DRP 425147) für die später als ENIGMA bekanntgewordene Maschine ebenfalls Antriebsräder mit ungleichmäßig verteilten Zähnen. Für die ENIGMA A von 1923 mit vier Rotoren war die unregelmäßige Rotorfortschaltung (patentiert für *Paul Bernstein*, angemeldet 26. März 1924, DRP 429 122) durch Verwendung von gezähnten Antriebsrädern mit Lücken so geregelt:

eines mit 5 Zähnen und 6 Lücken (11 Positionen),
eines mit 9 Zähnen und 6 Lücken (15 Positionen),
eines mit 11 Zähnen und 6 Lücken (17 Positionen),
eines mit 11 Zähnen und 8 Lücken (19 Positionen).

Es wurde so eine Periode von $11 \cdot 15 \cdot 17 \cdot 19$, also mehr als 50 000, erzielt, also etwa ein Neuntel von $\theta = 26^4 = 456\,976$ — immerhin auch noch fast eine progressive Chiffrierung.

Unregelmäßige Fortschaltung mittels Antriebsräder mit einer wechselnden Anzahl von Zähnen und Lücken wurde auch in der Chiffriermaschine (Farbtafel F) von *Alexander von Kryha* (Patentanmeldung vom 16. Januar 1925, DRP 434 642) benutzt; aber mit einer Periode von zwischen 260 und 520 war die Maschine kryptologisch sehr schwach. Der Mathematiker *Georg Hamel* pries in einem banalen Gutachten ihre Stärke.

Boris Hagelin, der *Damms* Firma *Aktiebolaget Cryptograph* übernahm, ersetzte 1935 die Halbrotoren durch einen ‚Stangenkorb‘, engl. *bar drum, lug cage*, der BEAUFORT-Chiffrierschritte bewirkte. Er benutzte weiterhin unregelmäßige Fortschaltung. In den Maschinen C-35/C-36 (Abb. 60a, Farbtafel G) wurde die Zahl der Antriebsräder auf fünf erhöht, die Periode betrug $17 \cdot 19 \cdot 21 \cdot 23 \cdot 25 = 3900225$. In der auf Rat von *Yves Gyldén* verbesserten Maschine C-38 wurden sechs Antriebsräder benützt, die Periode betrug nun $17 \cdot 19 \cdot 21 \cdot 23 \cdot 25 \cdot 26$, also knapp über 100 Millionen (Farbtafel H).[5] *Hagelin*

[5] Für Details siehe *Arto Salomaa*, Public-Key Cryptography, Berlin 1990, p. 44 ff.

erhielt von Frankreich eine Bestellung von 5 000 Maschinen, die von Ericsson-Colombes in Lizenz hergestellt wurden. Im 2. Weltkrieg wurden dann in den U.S.A. in Lizenz von Smith & Corona 140 000 Stück fabriziert, die bei der U.S.Army als M-209, bei der U.S.Navy als CSP 1500 geführt wurden (Farbtafel H). Eine unsichere C-38m wurde bei der italienischen Kriegsmarine im Mittelmeer verwendet. Spätere Hagelin-Maschinen haben eine Periode von $29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47$, d.h. über 2 Milliarden. BC 543 (Abb. 60b) war eine elektrisch angetriebene Variante (als C 41 in den letzten Kriegsjahren in Deutschland in den Wanderer-Werken nachgebaut).



Abb. 60a. C-35 nach B. C. W. Hagelin (A. B. Cryptoteknik, Stockholm)



Abb. 60b. BC 543 nach B. C. W. Hagelin (links) und deutscher Nachbau C 41 der Wanderer-Werke (rechts)

In den Nachkriegsjahren verbesserte *Boris Hagelin* seine Maschinen weiter. 1952 kam die Hagelin-Crypto CX-52 auf den Markt, die mit sechs Schlüsselrädern, ausgewählt aus zwölf, arbeitete (als H 54 in Lizenz von Hell gebaut).

8.5.3 Später, als Scherbius die Umkehrwalze eingeführt hatte und zu drei beweglichen Rotoren übergegangen war, gab er die besonderen Antriebsräder wieder auf und ersetzte sie durch Stoßklinken und Nuten auf den Rotorkörpern. Der schrittweise angetriebene ‚schnelle' Rotor R_N nahm bei

jeder vollen Umdrehung den ‚mittleren' Rotor R_M um einen Schritt mit; dieser wiederum bei jeder vollen Umdrehung den ‚langsamen' Rotor R_L. Dieser zählwerksartige ‚reguläre' Rotorantrieb war tatsächlich ein sehr regelmäßiger. (Die später eingeführten ‚Griechenwalzen' wurden nicht mitbewegt.) Die Periode betrug etwas weniger als die maximal erreichbare von $\theta = 26^3$, nämlich $26 \cdot 25 \cdot 26 = 16\,900$ (lediglich als Folge einer unzulänglichen mechanischen Konstruktion für die Mitnahme der Rotoren). Die Länge der Nachricht durfte nicht zu groß sein: Für die Wehrmachts-ENIGMA war zunächst vorgeschrieben, daß kein Spruch länger als 180 (ab 13.1.1940: 250) Zeichen sein durfte. Die ‚reguläre' Fortschaltung der Rotoren der ENIGMA I und der Wehrmachts-ENIGMA geschah dann durch Verwendung *einer* Nut an den *Einstellringen* der Rotoren.

Um wenigstens *etwas* Unregelmäßigkeit in die Übertragszählung zu bringen, wurden die Nuten bei den neuen Rotoren I bis V der Wehrmachts-ENIGMA an verschiedenen Stellen des Einstellringes angebracht (Farbtafel H):

Rotor	I	II	III	IV	V
Einstellbuchstabe	Y	M	D	R	H

Das war aber nur eine *complication illusionaire*, "*a complication that defeats itself*" nannte *Kahn* sie ironisch: Hätten alle Rotoren die Nuten beim selben Buchstaben gehabt, hätten die Kryptanalysten (bei bekannten Rotoren) nicht durch die Buchstaben, bei denen die Fortschaltung geschah, unterscheiden können, welcher Rotor als ‚schneller' Rotor eingesetzt war. Die Kriegsmarine merkte das anscheinend und legte die Nuten der beiden 1938 hinzugekommenen Rotoren VI und VII sowie die des 1939 eingeführten Rotors VIII an die gleichen Buchstaben. Diese Rotoren hatten im übrigen zwei Nuten, eine beim Einstellbuchstaben H, eine beim Einstellbuchstaben U.[6] Während bei der kommerziellen ENIGMA die Nut mit dem Rotorkörper verbunden war, war sie bei den Rotoren der Wehrmachts-ENIGMA mit dem Ring verbunden, damit der Rotorantrieb auch von der Ringstellung abhing.

Obwohl durch die zwei Nuten die Periode verkürzt wurde und die Gefahr einer *superimposition* (s. 19.1) wuchs – um sie zu bannen, wurde die Spruchlänge so drastisch beschränkt –, erschwerte diese kleine Unregelmäßigkeit die unbefugte Entzifferung. *Welchman* schrieb: "*We would have had great trouble if each wheel had had two or three turnover positions instead of one*". Übrigens hätten drei Nuten die Periode nicht verkürzt, da 3 und 26 relativ prim sind. Wurde das von OKW/Chi übersehen?

Eine Sonderausführung der ENIGMA für die unter *Wilhelm Canaris* stehende Abwehr besaß seltsamerweise kein Steckerbrett, wohl aber eine mitbewegte Umkehrwalze – es handelt sich also um eine echte Vier-Rotor-Maschine. Ein anderer Unterschied der Abwehr-ENIGMA zur ENIGMA D bestand in einem Rädertrieb zur Rotorbewegung anstelle der Nuten, beschrieben in einer Korn-

---

[6] Die Fortschaltung selbst ist erfolgt, wenn (um 19 Buchstaben versetzt) im Anzeigefenster R, F, W, K, A bzw. A oder N sichtbar werden. (In *Bletchley Park* gab es dazu den unsinnigen Merkspruch *Royal Flags Wave Kings Above*).

schen Patentanmeldung vom 9. 11. 1928, DRP 534 947 (U.S. Patent 1 938 028 von 1933). Die Abwehr-ENIGMA hatte neue Rotoren, deren Schaltnocken, wie die Nuten bei den Rotoren der Wehrmacht-ENIGMA, mit dem Einstellring verbunden waren. Die drei Rotoren hatten 11, 15 und 17 (und nicht 19, wie Twinn berichtete) Schaltnocken; sie bereiteten *Dillwyn Knox* deshalb viel Kopfzerbrechen, aber es gelang ihm trotzdem, im Herbst 1941 die Abwehr-ENIGMA zu brechen[7]. Die Zahnradkuppelung der Rotoren erlaubte in Verbindung mit einem Zählwerk ein Vorwärts- und Rückwärtskurbeln (Abb. 61).





Abb. 61. Rotor der Abwehr-ENIGMA von zwei Seiten, links mit Zahnkranz von 2×26 Zähnen, rechts mit Zahnpaaren als Schaltnocken

8.5.4 Die TYPEX (Type-X) der Briten, unter der Aufsicht einer Regierungskommission entwickelt und 1935, nach neun Jahren, fertiggestellt, ähnelte in mancher Hinsicht der Wehrmacht-ENIGMA; sie hatte zwar fünf Rotoren, von denen aber zwei — die am Eingang gelegenen — nicht fortgeschaltet wurden. Die Lampenanzeige war durch einen Streifendrucker ersetzt. Die TYPEX war insofern kryptanalytisch äquivalent einer 3-Rotor-ENIGMA mit einem nicht-involutorischen Steckerbrett. Wesentliche Unterschiede bestanden jedoch in der Fortschaltung. Sie war ebenfalls regulär, aber grundsätzlich mit mehreren Nuten pro Rotor. Der Nutenring war, wie bei der kommerziellen ENIGMA, fest mit dem Rotorring verbunden; der Rotorkörper (*'wiring slug'*) saß in einem Gehäuse, das den Rotorring trug und mit Einstellbuchstaben versehen war. Die Rotorkörper konnten in zweierlei Orientierungen R oder R^{-1} eingelegt werden. In einer typischen Ausführung konnten fünf Rotorkörper aus zehn ausgewählt werden. Es gab Ringe mit fünf, sieben und neun Nuten, im letzteren Fall waren die Nuten so angeordnet, daß die Mitnahme erfolgte, wenn im Anzeigefenster einer der Einstellbuchstaben B, G, J, M, O, R, T, V, X erschien. Nur Rotoren mit gleichen Nuten wurden zusammen gebraucht.

Die Rotoren der italienischen OMI konnten aus einem Gehäuse, das die Nuten enthielt, und einem Paar von Rotorkörpern zusammengebaut werden, sodaß man von 14 Rotoren, die je zu zweien zugleich fortgeschaltet wurde, oder von 7 Rotoren mit einer Auswahl aus $\binom{14}{2}=91$ Rotoren sprechen konnte (Abb. 62).

---

[7] *Knox* entwickelte an der Abwehr-ENIGMA eine epezielle Terminologie: Die gleichzeitige Fortschaltung von R_N und R_M nannte er 'crab', die von R_N,R_M und R_L 'lobster'.





Abb. 62. TYPEX Mark II (links) und
Rotormaschine der Ottica Meccanica Italiana (rechts)

Neben ENIGMAs gingen auch TYPEXs aus Restbeständen des 2. Weltkriegs nach 1945 in viele kleinere Länder; manche waren bis 1975 in Gebrauch.

Seit den späten 40er Jahren bis in die frühen 60er benutzte die North Atlantic Treaty Organization (NATO) in den U.S.A. entwickelte Rotor-Chiffriermaschinen für den multinationalen Gebrauch (man betrachtete die amerikanische SIGABA als zu gut, um mit anderen, kleinen Nationen geteilt zu werden). Die KL-7 (Abb. 63) besaß 5+2 Chiffrier-Rotoren; sie erinnerte im mechanischen Aufbau in mancher Weise an die britische TYPEX, sie hatte Plastik-Aufsteckringe, die die Mitnahme der Rotoren bewirkten. Die KL-7 war eine der letzten Rotormaschinen, die je produziert wurden. Die Sicherheit dieser Maschinen hatte sehr gut zu sein, da ihre Verfügbarkeit nicht auf die NATO-Mitglieder oder europäische Staaten beschränkt war. Hier zeigt sich erstmals deutlich die radikale Akzeptanz der Kerkhoffs'schen Mahnung und Shannonschen Maxime (s. 11.2.3), daß ein Chiffrierverfahren auch noch sicher sein muß, wenn das Gerät in gegnerische Hände gefallen ist. In der Tat hatte bereits 1962 der U.S. Offizier *Joseph G. Helmich* den Sowjets technische Informationen über Rotoren und Schlüssellisten verkauft; er wurde erst 1982 vom FBI verhaftet. Die Verwendung der KL-7 endete dann 1985 nach dem weiteren Spionagefall *Walker* – da war die Maschine ohnehin veraltet.

Das sowjetrussische Gegenstück zu den westlichen Rotormaschinen, eine 10-Rotor-Maschine, wurde von den Russen FIALKA („Veilchen“) genannt.

8.5.5 In den U.S.A. hatte sich der große *William Friedman* früh mit den Rotormaschinen von *Hebern*, der mit der U.S. Navy Kontakt hatte, beschäftigt und sie 1925 auch empfohlen. Bei einem Test der *Hebern*schen Maschine gelang *Friedman* ein Meisterstück: Es wurden ihm zehn Nachrichten der ungefähren Länge 300, alle mit der gleichen Rotorenanordnung chiffriert, vorgelegt und die Anfangsstellungen der Rotoren mitgeteilt. In zwei Wochen Arbeit gelang ihm die Lösung, die die Rekonstruktion der Verdrahtung mindestens einiger der Rotoren einschloß. Der dazugehörige Bericht wurde 1996 freigegeben, offenbar wurde *Friedmans index of coincidence* (s. 16.1) benutzt.



Abb. 63.
Rotormaschine KL-7
(Deckname ADONIS)

Die Navy unter *Laurence F. Safford* und die Army unter *Friedman* mit *Sinkov*, *Rowlett* und *Kullback* suchten jahrelang nach Verbesserungen der *Hebern*schen Maschine. *Hebern* hatte schließlich 1932 eine zufriedenstellende Maschine HCM mit fünf Rotoren und einigermaßen unregelmäßiger Fortschaltung. *Friedman*s Gruppe war jedoch damit nicht zufrieden.

Um 1935 entwarf *Friedman* selbst für das U.S. Army Signal Corps eine auf der ENIGMA aufbauende Maschine M-325, die wegen einiger praktischer Mängel zunächst ebenfalls nicht eingeführt wurde (sie wurde 1944 als SIGFOY gebaut). Dann wurde, wieder mit Nachdruck von der Navy, ECM Mark I, eine 5-Rotor-Maschine mit Stiftwalzen-Fortschaltung entwickelt, die endlich auch den höchsten Ansprüchen genügte. Jedoch gelang es *Frank Rowlett*, weitere Verbesserungen anzubringen, die zur ECM Mark II führten, oft lediglich ECM genannt, bei der Army auch M-134-C und SIGABA, bei der Navy CSP 889 (Abb. 64). Die SIGABA hat 15 Rotoren; fünf Chiffrierrotoren und fünf die einer unregelmäßigen Fortschaltung dienen, sitzen in einem entfernbaren Korb, weitere fünf sind in ihrer Wirkung einem Steckerfeld äquivalent. In den vierziger Jahren erwies sie sich als die sicherste Maschine der (westlichen) Welt. Sie war aber auch die teuerste – und die am besten bewachte. Das System war bis 1959 in Gebrauch. CCM ('*Combined Cipher Machine*'), auch als CSP-1700 bezeichnet, war eine hybride Maschine für Verbindungen mit SIGABA und TYPEX.

Aus der Maschine von Hebern entstand nach 1934 mit weiteren Verbesserungen durch professionelle Kryptologen die noch im 2. Weltkrieg eingesetzte '*Electric Cipher Machine*' ECM Mark III, die lange Zeit Verwendung fand, obwohl sie nicht den höchsten Ansprüchen an Sicherheit genügte.

8.5.6 Japan, auf dem Weg zur ostasiatischen Großmacht, konnte nach dem 1. Weltkrieg nicht mehr ohne Diplomatie und damit nicht mehr ohne Kryptologie auskommen. Seine Diplomaten benutzten, wie auch anderswo, Codebücher. Ein polnischer Berater, Hauptmann *Jan Kowalewski*, lehrte sie die einfachsten Sicherheitsmaßnahmen, wie etwa die russische Kopulation (3.4). Von 1919 bis Frühjahr 1920 führten die Japaner elf Codebücher ein, darunter



Abb. 64.
Rotormaschine ECM
(M-134-C SIGABA, CSP 889)

umfangreiche mit 25 000 Codegruppen. Die japanischen Funksprüche fanden naturgemäß das Interesse der *'Black Chamber'* des U.S. State Departments, die mit Unterstützung der Abteilung MI-8 des U.S. War Departments nach 1918 von *Herbert Osborne Yardley* (1889–1958) aufgebaut worden war. Offiziell war sie der *Military Intelligence Division* unterstellt, untergebracht war sie, unter strenger Abschirmung, in New York City; nach einem Einbruch bediente sie sich ab 1925 der Deckung einer *Code Compiling Company*, die auch tatsächlich den *Universal Trade Code* erstellte und vertrieb. *Yardley* und seine Leute waren recht fleißig und auch erfolgreich; im Sommer 1921 entzifferten sie ein Telegramm des japanischen Botschafters in London an sein Außenministerium, das delikate Informationen über die gerade in Vorbereitung befindliche Internationale See-Abrüstungskonferenz enthielt. Bis 1929 wurden insgesamt 45 000 Telegramme aus aller Herren Länder entziffert.

Am 4. März 1929 trat *Herbert C. Hoover* sein Amt als 31. Präsident der Vereinigten Staaten an, und manches änderte sich. *Hoover*s Blauäugigkeit ließ ihn und seinen *Secretary of State Henry L. Stimson* auf die anrüchigen Dienste der Entzifferer verzichten; die *Black Chamber* wurde zum 31. Oktober 1929 kurzerhand aufgelöst, die Unterlagen gingen an das Signal Corps der Army, das *Friedman* leitete. *Yardley* mußte sich eine andere Stellung suchen, fand aber auf dem Höhepunkt der Depression keine. Er mußte also Geld verdienen und entschloß sich in seiner Verbitterung und Not, ein Buch der Enthüllung und Abrechnung zu schreiben mit dem Titel "*The American Black Chamber*" (Indianapolis, 1931). *Yardley* war ein glänzender Geschichtenerzähler und das Buch wurde sogleich ein großer Erfolg. Er zog sich dadurch nicht nur den Zorn der Regierung zu – immerhin, meinte er zu seiner Rechtfertigung, habe das State Department die Interessen der Vereinigten Staaten sowohl durch die Auflösung der *Black Chamber* wie auch durch die Verwendung von "sixteenth-century codes" geschädigt, und die moralische Verurteilung der Aufdeckung stünde gerade dem State Department nicht zu. Er zog sich aber auch harte Kritik von Seiten seiner sachkundigen Kollegen zu, die besser als *Stimson* wußten, daß im Hinblick auf eventuelle kriegerische Verwicklun-

gen die nationalen Interessen nicht nur keinen Geheimnisbruch, sondern auch keine Unterbrechung der kryptologischen Kompetenz erlaubten.

Der Fall *Yardley* hatte ein parlamentarisches Nachspiel: Der 73. Congress der U.S.A. diskutierte 1933 kontrovers eine Gesetzesvorlage der Roosevelt-Administration, die die Veröffentlichung entzifferter Nachrichten strafbar machen sollte. Die Verfechter der Pressefreiheit unterlagen; *Public Law 37*, die *Lex Yardley*, ging in die Section 952, Title 18 des *United States Code*. *Yardley* selbst blieb von Strafverfolgung verschont.

Yardley hatte neunzehn Länder aufgezählt, deren diplomatische Codes kompromittiert waren; darunter elf süd-und mittelamerikanische sowie Liberia und China, was niemand wunderte; weiterhin England, Frankreich, Deutschland, Spanien und die Sowjet-Union, wo zumindest offiziös niemand moralischen Abscheu äußern konnte (man sagt, daß in den 20er Jahren jedes größere europäische Land seinerseits im Besitz eines oder mehrerer amerikanischer Codebücher war) – und Japan.

Das Buch wurde jedenfalls ein Riesenerfolg, 17 931 verkaufte Exemplare in den U.S.A., dazu weitere 5 480 in Großbritannien waren für ein Kryptologiebuch unerhörte Zahlen. Übersetzungen erfolgten ins Französische, Schwedische, Chinesische und – ins Japanische. Dort wurden sogar sensationelle 33 931 Exemplare verkauft, und das zeigt, daß *Yardley* den Nerv der japanischen Seele getroffen hatte.

Dort ließ sich sogar ein Abgeordneter zu harten Worten hinreißen, er sprach, das Außenministerium kritisierend, vom „Bruch des Vertrauens“, der diplomatische Konsequenzen haben müsse; der Außenminister und ehemalige japanische Botschafter in Washington zur Zeit der Internationalen See-Abrüstungskonferenz sprach von einer „Schande“. *Yardley* wurde beschimpft. Dabei hatte er Japan den größten Dienst erwiesen, zu dem er fähig war: Es war der Anstoß zu einer radikalen Verbesserung der kryptologischen Sicherheit in Japan. Um diese zu gewinnen, vervielfachten die japanischen Dienste ihre bereits begonnenen Anstrengungen auf maschinelle Chiffrierung.

Yardley wurde 1938 von *Chiang Kai-shek* angeheuert und brach japanische Spalten-Transpositionen. 1940 ging er nach Canada, wo er aber 1941, vermutlich auf britisch-amerikanischen Druck, durch den erprobt zuverlässigen *Oliver Strachey* ersetzt wurde.

8.5.7 Einem bewährten Muster folgend, studierten die Japaner die Maschinen anderer Länder, insbesondere die bereits durch die Patentliteratur zugängliche ENIGMA, die Maschinen von *Damm-Hagelin* und die Maschine von *Hebern*. Für Maschinen, die das lateinische Alphabet (*romaji*) verwendeten, wurde die gängige Transliteration von *Hepburn* benutzt. Der japanische Nachbau der ENIGMA D, von den Amerikanern GREEN genannt, war eine seltsam anmutende Konstruktion mit vier stehend angeordneten Rotoren (Abb. 65), er bekam keine größere Bedeutung. Die Halbrotoren von *Damm* fanden sich wieder in der von den Amerikanern RED genannten *angō kikai taipu A* („Chiffrier Maschine Typ A“). Sie hatte neben einer



Abb. 65. Japanischer ENIGMA-Nachbau, GREEN-Maschine

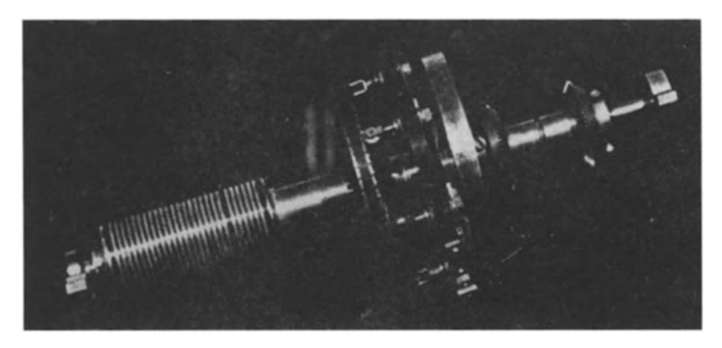


Abb. 66. Halbrotor mit 26 Schleifringen in der *angō kikai taipu A* (RED-Maschine)

festen Permutation durch ein Steckerfeld einen Halbrotor mit 26 Schleifringen (Abb. 66). Die Verdrahtung permutierte die sechs Vokale in sich und damit auch die 20 Konsonanten in sich und brauchte damit 60 Ausgangskontakte, da 60 das kleinste gemeinsame Vielfache von 6 und 20 ist. Der Grund für diese kryptologisch eher nachteilige Trennung lag vielleicht in den Tarifbestimmungen der internationalen Telegraphie. Die Fortschaltung geschah durch ein Antriebsrad mit einer 47-er Teilung, wobei 4, 5 oder 6 Stifte entfernt wurden und damit eine Unregelmäßigkeit erzielt wurde. Kryptologisch bewirkte *angō kikai taipu A* zwei separate ALBERTI-Chiffrierungen der Vokale und der Konsonanten; mit einer fast regulären Fortschaltung, nicht viel besser als die Maschine von Kryha. RED wurde bereits 1935 von *Kullback* und *Rowlett* von der U.S. Army angegriffen und 1936 vollständig rekonstruiert (im Nachbau wurden zwei Halbrotoren, einer mit 6, einer mit 20 Schleifringen verwendet, Abb. 67). Im Frühjahr 1936 machte sich bei Pers Z im Auswärtigen Amt *Werner Kunze* daran, eine über dem Kana-Alphabet arbeitende Variante, von den Amerikanern ORANGE genannt, aufzuklären,

es gelang ihm im September 1936. Bei der U.S.Navy löste diese Aufgabe *Jack S. Holtwick*. Auch in Großbritannien begann man noch vor Kriegsausbruch, die japanischen Chiffriermaschinen bis hin zu RED und ORANGE zu beherrschen.

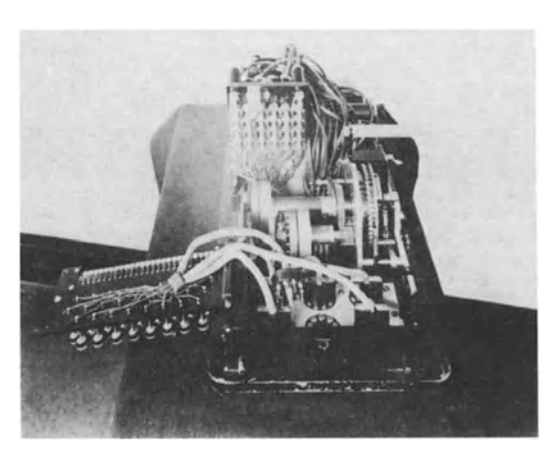


Abb. 67. Amerikanischer Nachbau RED der *angooki taipu A* mit zwei Halbrotoren

1937 begann Japan dann mit der Entwicklung einer wesentlich sichereren Chiffriermaschine, die 1939 eingeführt wurde – die erste aufgefangene, damit chiffrierte Nachricht ging im März 1939 von Warschau nach Tokio – und im diplomatischen Dienst die RED-Maschine ablöste. Die von den Amerikanern PURPLE genannte *angō kikai taipu B* (auch *97-shiki obun injiki*, Alphabetische Schreibmaschine, Jahr 2597 des japanischen Kalenders) zeigte ein neues, von den Japanern erstmals verwendetes Prinzip: Schrittschalter, die in der Vermittlungstechnik bekannt waren. Die Aufteilung in 6 und 20 Zeichen wurde beibehalten, obwohl später die sechs Zeichen nicht mehr ausschließlich Vokale sein mußten. Es standen nunmehr nur noch 25 Alphabete zur Verfügung, die allerdings auf komplizierte, durch Verdrahtung festgelegte Weise gebildet sind. Die Aufdeckung der inneren Struktur erforderte monatelange Arbeit einer ganzen Gruppe, zu der neben *Frank Rowlett Robert Ferner*, *Albert Small*, *Sam Snyder*, *Genevieve Feinstein (née Grotjan)*, *Mary Jo Dunning* gehörte. Sie gelang zunächst für die 6 Vokale, und es gab auch Anzeichen, daß 25 Alphabete im Spiel waren; für die 20 Konsonanten war jedoch keine Gesetzmäßigkeit in diesen Alphabeten zu erkennen – bis *Leo Rosen*, ein Neuling, mit einer Broschüre ankam, die einen Schrittschalter mit 25 Stellungen beschrieb (Abb. 68). Damit war der Durchbruch eingeleitet, ein Nachbau gelang, und im August 1940, nach 18 Monaten Arbeit, war PURPLE voll aufgedeckt. Im Januar 1941 bekamen die Briten in *Bletchley Park* einen PURPLE-Nachbau. Für den Erfolg war natürlich die enge Verwandtschaft zwischen RED und PURPLE entscheidend, und viele Schwachstellen in der Chiffrierdisziplin der Japaner gaben Anhaltspunkte, Hinweise und wahrscheinliche Phrasen, aber es war ein Sieg der U.S. Army Kryptanalysis über die Japaner "*that has not been duplicated elsewhere ... the British crypt-*

analytic service and the German cryptanalytic service were baffled in their attempts" (Friedman). In strategischer Hinsicht war der Bruch der PURPLE-Chiffrierung von höchster Bedeutung; die Amerikaner hatten für das so erhaltene Material das Codewort MAGIC. *Otto Leiberich* berichtet aber, daß auch die Deutschen PURPLE entzifferten. *David Kahn* glaubt zu wissen, daß sogar die Sowjetunion PURPLE brach.

Die Briten hatten aber fast zur gleichen Zeit auch ihren Triumph: ULTRA nannten sie ihr durch einen tiefen Einbruch in deutsche Kryptosysteme, darunter die ENIGMA der Wehrmacht, erhaltenes kostbares Material.

Sobald die PURPLE-Maschine rekonstruiert war, bot sie übrigens keineswegs mehr Sicherheit als RED. Man kann den Eindruck gewinnen, daß die Japaner die Geschicklichkeit der Amerikaner unterschätzten und daß sie glaubten, ihre Sprache biete allein schon einen gewissen Schutz und würde anderswo nicht so leicht verstanden. Mit Schrittschaltern bauten die Japaner weitere Typen: Eine, die die Amerikaner CORAL nannten, hatte nunmehr die Aufteilung 20+6 aufgegeben (sie wurde von OP-20-GY Mitte März 1944 gebrochen), eine andere, JADE, die mit 50 Zeichen, davon 24 häufige und 24 seltene Kana-Zeichen, arbeitete (sie war nur unwesentlich verschieden von CORAL und wurde ebenfalls bald gebrochen).

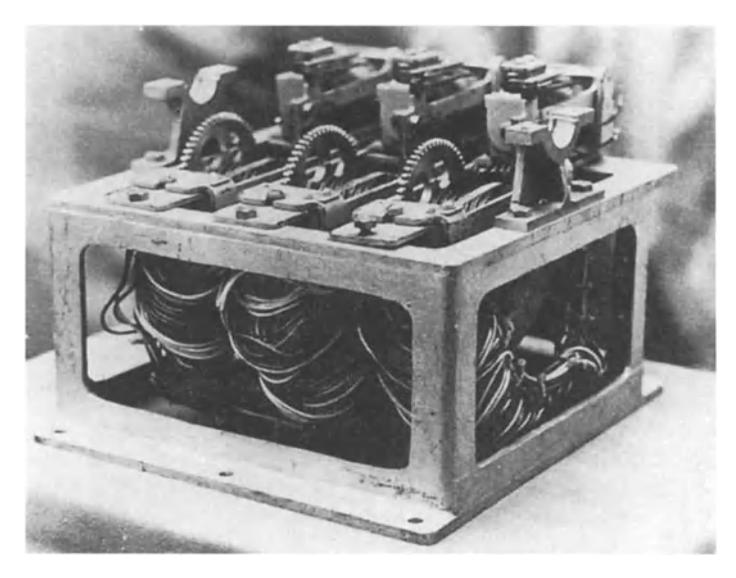


Abb. 68. Schrittschalter-Bank aus der japanischen PURPLE-Maschine

Die Japaner hatten auch eine sehr durchsichtige Systematik in ihren täglichen Steckerbrett-Anordnungen und die schlechte Gewohnheit, Änderungen in ihren Chiffrieranweisungen stets als chiffrierte Nachrichten zu übermitteln – wodurch der Gegner, sobald ihm einmal ein Einbruch gelungen war, stets bestens informiert blieb. *Frank Raven* entdeckte 1941 sogar einen Schlüssel zu den Schlüsseln: jeweils ein Satz von zehn gleichbleibenden Permutationen.

8.6 Bildung von Schlüsselfolgen durch Iteration

8.6.1 Für VIGENÈRE- und BEAUFORT-Verfahren braucht man allgemein ‚unregelmäßige' Folgen von Zykelzahlen aus $\mathbb{Z}_N$. Eine gebräuchliche Methode hierfür benutzt sukzessive Potenzen *modulo* N einer k-reihigen regulären, von der Identität verschiedenen Matrix T. Da die Anzahl solcher Matrizen (vgl. 5.2.3) höchstens N^{k^2} beträgt, muß eine gewisse Potenz T^r erstmals die Identität ergeben. $r = r(T, N)$ heißt Ordnung der Matrix T in $\mathbb{Z}_N$.

Beispielsweise hat die Matrix $T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ mit $k = 2$ in Abhängigkeit von N folgende Ordnung r

$N=$	2	3	4	5	6	7	8	9	10	11	12	13	16	20	23	24	25	26	32	48	64	80	160
$r=$	3	8	6	20	24	16	12	24	60	10	24	28	24	60	48	24	100	84	48	24	96	120	240

(siehe auch 9.4.2). Greift man ein geeignetes i-j-Element der Matrixpotenzen heraus, so erhält man eine Folge von Zykelzahlen mit der Periode $r(T, N)$.

Speziell eignet sich für T eine k-reihige ‚Begleitmatrix' der Form

$$A = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & \alpha_k \\ 1 & 0 & 0 & \dots & 0 & \alpha_{k-1} \\ 0 & 1 & 0 & \dots & 0 & \alpha_{k-2} \\ & & \vdots & & & \\ 0 & 0 & 0 & \dots & 0 & \alpha_2 \\ 0 & 0 & 0 & \dots & 1 & \alpha_1 \end{pmatrix}$$

Das 1-k-Element der Potenzen dieser Matrix ergibt sich dann als letztes Element des iterierten Vektors $t_i = t_0 A^i = t_{i-1} A$, wenn man beginnt mit $t_0 = (1\ 0\ 0\ \dots\ 0\ 0)$.

Zur Bildung dieser iterierten Vektoren benutzt man ein **Schieberegister** mit k Plätzen. Schieberegister in Verbindung mit einer Begleitmatrix heißen auch **lineare Schieberegister**. Sie bieten über eine Basisanalyse leichte Einbruchmöglichkeiten (s. 20.3). Bei nichtlinearen Schieberegistern erfolgt die Bildung des jeweils nächsten Wortes der Folge durch eine *beliebige* Funktion.

Einfache Maßnahmen zur Einführung einer Nichtlinearität, wie etwa das Umdrehen der Reihenfolge der Komponenten nach jedem Schritt, sind gefährlich: Sie können sogar zu einer Verkürzung der Periode führen (*Selmer* 1993, *Brynielsson* 1993).

8.6.2 Für den binären Fall $N{=}2$ handelt es sich um $(0, 1)$-Folgen. Beispielsweise ergibt die Matrix $(k = 3)$

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

modulo 2 die Folge $(0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\ \dots)$ der Periode $7 = 2^3 - 1$. Da es 2^k verschiedene k-Bit-Vektoren gibt, und der Nullvektor

in sich übergeht, ist klar, daß 2^k-1 die maximale so erzielbare Periode ist. Es läßt sich zeigen (*Oystein* 1948):

Wenn das Polynom $x^k - \alpha_1 x^{k-1} - \alpha_2 x^{k-2} - \ldots - \alpha_k$ im Körper $\mathbb{Z}_2 = GF(2)$ irreduzibel ist, so hat jede mit A iterierte Vektorfolge eine Periode, die ein Teiler von 2^k-1 ist.[8]

Ist 2^k-1 prim (2^k-1 heißt dann Mersenne-Primzahl[9]), so gibt es nur die Perioden 2^k-1 und 1; zu letzterer gehört die triviale Folge $(0\ 0\ 0\ 0\ \ldots)$.

Für $N{=}2$, also in $\mathbb{Z}_2$, gibt es nur zwei Permutationen und keine zweigliedrige Rotorfamilie. Es verbleiben nur die VIGENÈRE- und BEAUFORT-Schritte **+O** und **+L**, d.h. die VERNAM-Schritte $O \mathrel{\hat{=}} 0$ und $L \mathrel{\hat{=}} 1$. Polyalphabetische *binäre* Chiffrierung erfordert besonders eine hohe Periode und einen guten Mechanismus zur Erzielung einer ‚unregelmäßigen' $(0,1)$-Folge.

8.6.3 Grundsätzlich kann man aus jeder Menge monoalphabetischer Block-Chiffrierschritte χ_i mit einheitlicher Chiffrierbreite m, die dabei sehr groß sein kann, eine endliche Folge (vgl. 2.3) $X = (\chi_{i_1}, \chi_{i_2}, \ldots, \chi_{i_s})$ bilden und X auf einer Ausgangsnachricht $u = (u_1, u_2, \ldots, u_s)$ iterieren; die progressive Folge

$$u\ ,\ X(u)\ ,\ X^2(u)\ ,\ X^3(u)\ ,\ \ldots$$

wird zwar periodisch, aber meistens von sehr großer Periode.[10] Beispielsweise wird in 9.5.2 X als h-te Potenz *modulo* einer Primzahl p definiert,

$$X(u) = u^h \bmod p\ ,\ X^s(u) = u^{(h^s)} \bmod p\ .$$

8.7 Nichtperiodische Schlüssel

Eine nichtperiodische Chiffrierung (2.3.6) erfordert $\theta \geq 2$ und eine nichtperiodische Folge $(\chi_{i_1}\ ,\ \chi_{i_2}\ ,\ \chi_{i_3}\ \ldots)$ von Chiffrierschritten. Sie wird charakterisiert durch die Indexfolge $(i_1\ ,\ i_2\ ,\ i_3\ ,\ \ldots)$ mit $0 \leq i_\mu < \theta$, oder durch den echten Bruch $.i_1 i_2 i_3 \ldots$ im Zahlsystem zur Basis $\theta \geq 2$. Damit gibt es zu jeder irrationalen reellen Zahl und jedem θ eine nichtperiodische Chiffrierung.

8.7.1 Eine nichtperiodische Chiffrierung wie etwa (für $\theta = 2$) eine mit der *unendlichen* Indexfolge (dem ‚fortlaufenden Schlüssel')

$$(\,1\,1\,0\,1\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\ \ldots)$$

---

[8] Für $k = 31$ ist das Polynom $x^{31} + x^{13} + 1$ irreduzibel, die zugehörige Periode $2^{31}-1$ beträgt über 2 Milliarden.

[9] Dies ist der Fall für $k = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$. Die Primalität von $2^{61}-1$ wurde erst 1883 von *Pervusin* bewiesen, die Primalität von $2^{127}-1$ schon 1876 von *Lucas*. Mit Hilfe der SWAC wurden 1952 von *Ralph M. Robinson* $2^{521}-1$, $2^{607}-1$, $2^{1279}-1$, $2^{2203}-1$, $2^{2281}-1$ als prim nachgewiesen. Weitere 14 folgten, dann $2^{756839}-1$ (1992), $2^{859433}-1$ (1994), $2^{1398269}-1$ (1996), $2^{2976221}-1$ (1997), $2^{3021377}-1$ (1998), $2^{6972593}-1$ (1999) — eine Verzehnfachung des Exponenten in 7 Jahren.

[10] Nach *Robert Floyd* kann man mit hohem Rechenaufwand, aber mit minimalem Speicheraufwand die Periode von X folgendermaßen feststellen: Sei $a_0 = u$, $b_0 = u$ und $a_{i+1} = X(a_i)$, $b_{i+1} = X^2(b_i)$. Sobald $a_n = b_n$, ist $X^n(u) = X^{2n}(u)$ und n ist die Periode.

d.h. $i_\mu = \begin{cases} 1 & \text{falls} \quad \mu = 2^k \\ 0 & \text{sonst} \end{cases}$

bringt gegenüber einer periodischen Chiffrierung keinen Vorteil.

Aber auch eine fortlaufende Chiffrierung mit der Indexfolge der ‚Mephisto-Polka' (*Axel Thue* 1904, *Marston Morse* 1921), wie sie von *Max Euwe* schon 1929 benützt wurde,

(1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 0 ...)

hat ein einfach zu durchschauendes Bildungsgesetz des Schlüssels, das eine rekursive Berechnung erlaubt. Und die fraktale Wortfolge

$$
\begin{aligned}
a_0 &\mathrel{\hat{=}} (0)\\
a_1 &\mathrel{\hat{=}} (1)\\
a_2 &\mathrel{\hat{=}} (0\ 1)\\
a_3 &\mathrel{\hat{=}} (1\ 0\ 1)\\
a_4 &\mathrel{\hat{=}} (0\ 1\ 1\ 0\ 1)\\
a_5 &\mathrel{\hat{=}} (1\ 0\ 1\ 0\ 1\ 1\ 0\ 1)\\
a_6 &\mathrel{\hat{=}} (0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1)\\
a_7 &\mathrel{\hat{=}} (1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1)\\
&\vdots
\end{aligned}
$$

die durch das Lindenmayer-Ersetzungssystem (*Aristide Lindenmayer*, 1968)

$$\begin{cases} 0 \to 1 \\ 1 \to 0\ 1 \end{cases}$$

erzeugt wird, hat ebenfalls ein durchschaubares Bildungsgesetz: es ist für $i \geq 2 \quad a_i = a_{i-2} \circ a_{i-1}$.

Wie kommt man zu einer ‚unregelmäßigen' nichtperiodischen Indexfolge, die ja dem Chiffrierer und dem Dechiffrierer bekannt sein muß, auf bequeme Weise?

Auf die Idee, als Schlüssel einen Text aus einem weit verbreiteten Buch zu nehmen, kommen vor allem Amateure immer wieder, aber eingedenk der Grundregel „der Feind kennt das benutzte System" ist das ein *festes* Verfahren, mit allen schon in 2.6.1 aufgeführten Gefahren. Für verständliche Schlüsseltexte in einer geläufigen Sprache gibt es ein systematisches Zick-Zack-Verfahren (14.4), das bei Shannonschen Chiffrierschritt-Systemen mit bekannten Alphabeten (2.6.4) anwendbar ist.

8.7.2 Es darf also nicht verwundern, daß schon frühzeitig Möglichkeiten ersonnen wurden, einen nichtperiodischen Schlüssel aus dem Klartext selbst abzuleiten. Der entscheidende Schritt kommt von *Geronimo Cardano* (1501–1576). Nachdem *Belaso* polyalphabetische Substitutionen mit Schlüsseln eingeführt hat, geht *Cardano* in seinem Buch *De Subtilitate* 1550 so vor, daß er, für jedes Wort neu beginnend, den Klartext von Anfang an benutzt:[11]

[11] Alphabet $Z_{20} \cup \{x, y\}$, Chiffrierung linear polyalphabetisch mit

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	v	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

.

s	i	c	e	r	g	o	e	l	e	m	e	n	t	i	s	
S	*I*	*C*	*S*	*I*	*C*	*E*	*S*	*I*	*C*	*E*	*R*	*G*	*O*	*E*	*L*	.
N	T	F	Z	C	L	T	Z	V	H	R	Y	V	I	P	E	

Die Idee (engl. *autokey*, frz. *autoclave*, *autochiffrant*) war gut gemeint, ja sogar bestechend; aber *Cardano* hat wohl selbst nie die Dechiffrierung versucht: Die Chiffrierung des Startwortes mit sich selbst als Schlüssel ist nämlich nicht eindeutig umkehrbar: s und *S* wie auch f und *F* ergeben N; i und *I* wie auch x und *X* ergeben T; c und *C* wie auch p und *P* ergeben F etc. Der unbefugte Dechiffrierer hat nicht mehr Arbeit, die richtige Kombination unter 2^k Kombinationen (wenn das erste Wort k Buchstaben hat) herauszufinden, als der berufene Dechiffrierer. *Belaso* suchte den Mangel zu beheben, indem er das erste Wort nach *Trithemius* chiffrierte und für jedes weitere Wort einen progressiven Schlüssel, beginnend mit dem Anfangsbuchstaben des vorhergehenden Wortes, benutzte:

s	i	c	e	r	g	o	e	l	e	m	e	n	t	i	s	
A	*B*	*C*	*S*	*T*	*V*	*X*	*E*	*F*	*G*	*H*	*I*	*L*	*M*	*N*	*O*	.
T	M	E	Z	N	D	M	L	R	N	V	P	Z	G	Y	H	

Aber das war immer noch ein festes Verfahren. *Vigenère* hatte dann die rettende Idee, doch einen frei wählbaren **Schlüsselkeim** (*'priming key'*) ins Spiel zu bringen: Er wählte den ersten Buchstaben des Schlüssels frei und nahm sodann als weitere Schlüsselbuchstaben entweder die des Klartextes oder die des Geheimtextes (*'autokey'*):

a	u	n	o	m	d	e	l	e	t	e	r	n	e	l
D	*A*	*U*	*N*	*O*	*M*	*D*	*E*	*L*	*E*	*T*	*E*	*R*	*N*	*E*
X	I	A	H	G	U	P	T	M	L	S	H	I	X	T

a	u	n	o	m	d	e	l	e	t	e	r	n	e	l
D	*X*	*H*	*E*	*E*	*C*	*O*	*U*	*M*	*X*	*G*	*N*	*A*	*B*	*Q*
X	H	E	E	C	O	U	M	X	G	N	A	B	Q	O

Die polyalphabetische Chiffrierung über Z_{20} (Abb. 69) war dabei involutorisch, ähnlich *Porta* (Abb. 53), und nicht à la VIGENÈRE.

Die zweite Art ist allerdings unbrauchbar: Der Schlüssel ist vollständig exponiert, die ganze Nachricht kann bis auf das erste Zeichen sofort entschlüsselt werden (*Shannon* 1949). Nur wenig besser ist es beim rekurrenten Verfahren der ersten Art: Man muß den Anfangsbuchstaben des Schlüssels kennen, um weiterzukommen. Die zwei Dutzend Möglichkeiten sind allerdings schnell durchprobiert. Das wird besser, wenn nicht nur der erste Buchstabe, sondern d Schlüsselbuchstaben als Anfang vorgegeben werden. Die kombinatorische Komplexität ist allerdings nicht anders als die einer Chiffrierung mit einem periodischen Schlüssel der Länge d. Zwar ist bei hinreichend langem Anfang kein Durchprobieren mehr möglich, aber die ersten d Zeichen werden, wenn man den gleichen Anfang wiederholt verwendet, in einer Reihe von Nachrichten mit dem gleichen Schlüssel chiffriert; das kann zum Einbruch genügen.

Nachteilig ist insbesondere die Verschleppung von Chiffrierfehlern bei diesem Verfahren — generell eine Schwäche aller *autokey*.

A B	↕	a	b	c	d	e	f	g	h	i	l
		m	n	o	p	q	r	s	t	u	x
C D	↕	a	b	c	d	e	f	g	h	i	l
		x	m	n	o	p	q	r	s	t	u
E F	↕	a	b	c	d	e	f	g	h	i	l
		u	x	m	n	o	p	q	r	s	t
G H	↕	a	b	c	d	e	f	g	h	i	l
		t	u	x	m	n	o	p	q	r	s
I L	↕	a	b	c	d	e	f	g	h	i	l
		s	t	u	x	m	n	o	p	q	r
M N	↕	a	b	c	d	e	f	g	h	i	l
		r	s	t	u	x	m	n	o	p	q
O P	↕	a	b	c	d	e	f	g	h	i	l
		q	r	s	t	u	x	m	n	o	p
Q R	↕	a	b	c	d	e	f	g	h	i	l
		p	q	r	s	t	u	x	m	n	o
S T	↕	a	b	c	d	e	f	g	h	i	l
		o	p	q	r	s	t	u	x	m	n
U X	↕	a	b	c	d	e	f	g	h	i	l
		n	o	p	q	r	s	t	u	x	m

Abb. 69. Involutorische polyalphabetische Chiffrierung von *Vigenère*

Babbage erfand den *autokey* wieder — diesmal sogar mit einem permutierten Alphabet — und gab dann auch ein Verfahren an, ihn zu brechen. Erst *Shannon* scheint 1949 bemerkt zu haben, daß rekurrentes VIGENÈRE-Verfahren zu VIGENÈRE-Verfahren der Periode 2 ähnlich ist. Wird der Klartext in Gruppen $a_1\ a_2\ a_3\ \ldots$ der jeweiligen Länge d abgeteilt und ist D der Schlüsselkeim, so gelten für den Geheimtext $C_1\ C_2\ C_3\ \ldots$ (Stelle für Stelle *mod.* N) die Beziehungen

$$C_1 = a_1 + D, \qquad C_i = a_i + a_{i-1} \qquad (i = 2,\ 3,\ \ldots)$$

und somit die rekurrenten Beziehungen

$$\begin{aligned} C_1 &= a_1 + D \\ C_2 - C_1 &= a_2 - D \\ C_3 - C_2 + C_1 &= a_3 + D \\ C_4 - C_3 + C_2 - C_1 &= a_4 - D \quad \text{usw., die Folge} \end{aligned}$$

$$C_1\ ,\ C_2 - C_1\ ,\ C_3 - C_2 + C_1\ ,\ C_4 - C_3 + C_2 - C_1\ ,\ \ldots$$

läßt sich also behandeln wie ein polygraphisches VIGENÈRE-Verfahren der Periode 2, d.h. wie zwei alternierende polygraphische CAESAR-Additionen.

Auch die Verwendung eines permutierten Alphabets ändert daran nichts. Entsprechendes gilt für rekurrentes BEAUFORT-Verfahren.

8.7.3 Bei den Chiffrier-Fernschreibern T52d, T52e von Siemens und SZ42 von Lorenz konnte, wie schon 1920 von *Damm* vorgeschlagen (*'influence letter'*), die ‚unregelmäßige' Fortschaltung vom Klartext beeinflußt werden („mit Klartextfunktion"), die Chiffrierung war damit praktisch nichtperiodisch. Bei gestörten Leitungen führte das allerdings zu einem ‚Außer-Tritt-Fallen' der Chiffrierung; die Klartextfunktion wurde deshalb, zur Erleichterung der britischen Entzifferer, nur wenige Monate Ende 1944 gebraucht.

8.7.4 Besser als die rekurrenten Chiffrierungen der Art $c_i = f(p_i, p_{i-1})$, die *Vigenère* und *Babbage* benutzten, ist eine **Stromchiffrierung** (*stream cipher*) $c_i = X(p_i, k_i)$, eine schließlich periodische Chiffrierung, bei der die unendliche Schlüsselfolge k_i durch einen endlichen Automaten G als **Schlüsselerzeuger** (engl. *key generator*), $k_i = G(k_{i-1}, p_{i-1})$, gewonnen wird; mit k_1 als Schlüsselkeim (*priming key*).

8.8 Individuelle Einmal-Schlüssel

8.8.1 Nachdem einfache rekurrente Chiffrierverfahren nichts bringen, verbleibt noch, Sender und Empfänger mit einem theoretisch unbegrenzten Vorrat eines *fortlaufenden*, echt unregelmäßigen, sinnlosen und zufälligen, nur ein einziges Mal vorhandenen und zu gebrauchenden ‚individuellen' Schlüsels auszurüsten. Diese Idee, von *Vernam* 1918 eher nebenbei geäußert, griff zwischen den Weltkriegen rasch um sich; in den U.S.A., in der Sowjetunion und in Deutschland gibt es frühe Spuren.

8.8.2 *Joseph O. Mauborgne*, der später Major General und Chief Signal Officer, U.S. Army (1937–1941) wurde, hatte *Parker Hitts* Mahnung von 1914 im Ohr – *"no message is safe in [the Larrabee] cipher unless the key phrase is comparable in length with the message itself"* – und führte an Hand der VERNAM-Maschine (8.3) den **Einmal-Schlüssel** (engl. *one-time tape, one-time pad*, OTP) ein, der, über Morehouse (8.3.2) hinausgehend, ein völlig unregelmäßiger, aperiodischer **individueller Schlüssel** (im Jargon ‚i-Wurm') sein sollte.[12]

In Deutschland propagierten *Kunze*, *Schauffler* und *Langlotz* schon 1921 Blöcke mit 50 Blättern, die je 240 Ziffern (in 48 Gruppen von Fünfen) enthielten, zur Überschlüsselung numerischer Codes. Das Auswärtige Amt verwendete seit 1926 regelmäßig Überchiffrierung (9.2.1) durch Einmal-Schlüssel.

Auch die Sowjets gingen 1926 zum Gebrauch individueller Schlüssel über, sehr zum Leidwesen von *Fetterlein*, dem Spezialisten für die Sowjetunion

[12] Einmal-Schlüssel sollte man also bestimmungsgemäß nach Gebrauch sofort vernichten. Bei VERNAM-Geräten kann das maschinell geschehen, beim Siemens Schlüsselfernschreiber SFM T 43 geschah es auf diese Weise.

im britischen M.I.1(b). Die Sowjets behielten eine Vorliebe für individuelle Schlüssel; Farbtafel O zeigt ein russisches Blatt, bei einem Spion aufgefunden.

Eine große praktische Schwierigkeit liegt darin, genügend Schlüsselmaterial für umfangreichen Nachrichtenverkehr zur Verfügung zu stellen, insbesondere in instabilen Situationen auf dem Schlachtfeld. Diese Schwierigkeiten sind eher zu bewältigen bei höheren Stäben des Militärs, bei diplomatischen Vertretungen, und im rein zweiseitigen Nachrichtenverkehr mit Spionen; in solchen Situationen werden individuelle Einmal-Schlüssel für Nachrichten der höchsten Sicherheitsstufe häufig benützt, vorausgesetzt der Schlüsselnachschub kann nicht abgeschnitten werden.

8.8.3 Die Ziffernfolgen oder Zeichenfolgen sollten natürlich keinerlei Gesetzmäßigkeit genügen, sondern ‚zufällig‘ sein. Gute stochastische Quellen für (Pseudo-)Zufallszahlenfolgen sind aber teuer. Dazu bemerkt *Kahn* (über russische individuelle Schlüssel):

> *Interestingly, some pads seem to be produced by typists and not by machines. They show strike-overs and erasures — neither likely to be made by machines. More significant are statistical analyses of the digits. One such pad, for example, has seven times as many groups in which digits in the 1-to-5 group alternate with digits in the 6-to-0 group, like 18293, as a purely random arrangement would have. This suggests that the typist is striking alternately with her left hand (which would type the 1-to-5 group on a Continental machine) and her right hand (which would type the 6-to-0 group). Again, instead of just half the groups beginning with a low number, which would be expected in a random selection, three quarters of them do, possibly because the typist is spacing with her right hand, then starting a new group with her left. Fewer doubles and triples appear than chance expects. Possibly the girls, ordered to type at random, sensed that some doublets and triplets would occur in a random text but, misled by their conspicuousness, minimized them. Despite these anomalies, however, the digits still show far too little pattern to make cryptanalysis possible.*

8.8.4 Stammt der individuelle Schlüssel aber aus einer stochastischen Quelle, die alle Zeichen mit gleicher Wahrscheinlichkeit und voneinander unabhängig abgibt, so gilt der damit chiffrierte Geheimtext als ‚unbrechbar‘ (engl. *holocryptic*[13]). Was damit intuitiv gemeint ist, scheint auf den ersten Blick klar zu sein; es wird sich auch lohnen, in der Kryptanalysis zu verfolgen, wie sämtliche Lösungsmethoden an Voraussetzungen gebunden sind, die nach der zu gebenden Definition verletzt sind. Das ist jedoch kein Beweis; in der Tat geht es um eine geeignete präzise Formulierung von ‚unbrechbar‘. Sie muß stochastischer Natur sein. Am deutlichsten hat, auf *A. N. Kolmogorov* zurückgreifend, 1974 *Gregory J. Chaitin* eine solche vorgezeichnet. Ihm und *Claus-Peter Schnorr* (1970) folgend verlangen wir, daß für die unendliche Indexfolge einer nichtperiodischen, fortlaufenden Chiffrierung, die ‚unbrechbar‘ genannt werden soll, gilt:

> *Für jede endliche Teilfolge gibt es keine kürzere algorithmische Beschreibung als die Auflistung der Teilfolge — keine Teilfolge ist in eine kürzere Beschreibung ‚komprimierbar‘.*

---

[13] Den Ausdruck verwendete schon *Pliny Earle Chase* 1859.

Damit scheiden als unendliche Indexfolgen alle Ziffernfolgen aus, die durch einen festen Algorithmus, also maschinell, erzeugt werden, insbesondere alle rationalen oder irrationalen Zahlen (8.7) – sofern sie berechenbar sind.[14]

Nicht-berechenbare reelle Zahlen gibt es immer noch überabzählbar viele. Ob aber zu jeder von ihnen eine ‚unbrechbare' fortlaufende Chiffrierung gehört, ist nicht bekannt.

8.8.5 Physikalische Effekte, die heute zur Erzeugung „echter" nichtperiodischer zufälliger Schlüssel dienen können, beruhen auf der Überlagerung inkommensurabler Schwingungen oder auf chaotischen nichtlinearen Systemen. Sie sind anscheinend zuverlässiger als die um 1950 benutzten Rauscheffekte von Röhren und Zener-Dioden oder Geigerzähler-Aufzeichnungen. Röhrenrauschen wurde bereits 1943 benutzt zur Herstellung individueller Schlüssel für das britische ROCKEX-System, eine VERNAM-Chiffrierung, die dem hochgesicherten Verkehr der Briten mit den USA – etwa eine Million Wörter pro Tag, heute der Inhalt von vier 3.5″·2HD-Disketten pro Tag – diente.

8.8.6 Die Wehrmacht führte 1943 für die höchste Führungsebene[15] Fernschreibmaschinen mit angebautem Lochstreifenleser für individuelle Einmal-Schlüssel ein (Siemens Schlüsselfernschreibmaschine T 43, mit Blattschreiber T typ 37f). Sie wurden 1944 zwischen der Funkfernschreibstelle Golßen bei Berlin und einigen Heeresgruppen sowie dem Führerhauptquartier in Ostpreußen als Ersatz für SZ 42 eingesetzt. Nach dem 20. Juli 1944 wurde die Funkfernschreibstelle des OKH in die Bunker bei Zossen verlegt, im Herbst wurde sie nach Freilassing in Oberbayern, in die angebliche ‚Alpenfestung', ausgelagert. Es kamen kaum mehr als zwei Dutzend Maschinen zum Einsatz.



Abb. 70. Siemens Schlüsselfernschreibmaschine T 43, mit Blattschreiber T typ 37f

[14] Zahlen wie $\sqrt{2}$, $\sqrt{5}$, $\sqrt{17}$ sind ohnehin ungeeignet: Sie können zu leicht erraten werden.
[15] Vermutlich identisch mit der in BP THRASHER (Fuchshai) genannten Machine.

Das U.S. State Department begann 1944 für seine höchst geheimen Nachrichtenverbindungen SIGTOT zu gebrauchen, ein VERNAM-Kryptosystem der U.S. Army mit individuellen Einmal-Schlüsseln. Die Army benutzte auch M-134-A (SIGMYC), eine 5-Rotor-Chiffriermaschine, deren Rotoren durch einen individuellen 5-Kanal-Lochstreifen bewegt wurden. Das VERNAM-System wurde im Januar 1943 durch ein Rotor-System M-228 (SIGCUM) ersetzt, das von *Friedman* entworfen worden war. *Rowlett* fand jedoch nach einigen Tagen eine ernste Schwäche des Systems, das daraufhin aus dem Verkehr gezogen bzw. im April 1943 durch eine verbesserte Version ersetzt wurde.



Gilbert Vernam (1890–1960)

Nur eine Handvoll Nachkriegs-Kryptosysteme auf dem offenen Markt waren Einmal-Schlüssel-Systeme, darunter sind zu erwähnen Mi-544 von Standard Elektrik Lorenz in Deutschland und die Hagelin T-52 und T-55 der Crypto AG in Zug (Schweiz). Die Sowjets nannten ihre Einmal-Schlüssel-Maschine AGAT (‚Achat').

8.8.7 Problematisch ist auch, was der Begriff *Einmal-Schlüssel* praktisch bedeutet. *Hüttenhain* berichtet, daß im Auswärtigen Amt nach den Sicherheitsvorschriften von jedem Blatt nur das Original und *eine* Kopie existieren sollte. Tatsächlich wurden neun Kopien hergestellt und an fünf diplomatische Vertretungen gesandt.

Mehrfachverwendung von Einmal-Schlüsseln erlaubte Cecil Phillips (1925–1998), Richard Hallock, Genevieve Feinstein und Lucille Campbell ab Herbst 1943 erfolgreiche Angriffe auf das höchste sowjetische Chiffriersystem ("Venona breaks"). Dieser Bruch brach später Julius und Ethel Rosenberg das Genick und enttarnte schließlich Harold Philby, Donald Maclean und Guy Burgess, Klaus Fuchs und Pierre Cot als Spione. 1946 wurden die Sowjets durch William Weisband und um 1949 durch Philby gewarnt, was sie möglicherweise veranlaßte, nach 1949 keine duplizierten Einmal-Schlüssel zu gebrauchen.

Eine klare Verletzung der Idee einer unbrechbaren Chiffrierung ist die Herstellung von Schlüsselfolgen durch eine Maschine. Wenn dann ein Geheimtext-Geheimtext-Kompromiß vorkommt zwischen einem solchen System und einem, sagen wir einmal, System, das Additive periodisch verwendet und wenn das letztere, was nicht unmöglich ist, gebrochen wird, so liegt der angeblich zufällige Einmal-Schlüssel offen. Falls genügend solches Material anfällt, kann die Maschine, die die Schlüsselfolge herstellte, rekonstruiert werden. Dies geschah tatsächlich im Falle der deutschen diplomatischen Chiffre, die die Briten FLORADORA nannten (9.1.1): Der angeblich zufällige Einmal-Schlüssel zeigte eine Gesetzmäßigkeit: *Erich Langlotz* auf der deutschen Seite kannte *Chaitin*s Doktrin noch nicht. Bletchley Park konnte sogar herausfinden, welche Maschine involviert war — nach *P. W. Filby* berichtete ihm *Nigel de Grey*, ein *Mr. Lorenz* habe 1932 dem *Foreign Office* eine solche angeboten.

8.9 Schlüsselverwaltung

8.9.1 Die einzelnen Zeichen eines Schlüssels dienen der Bildung oder Auswahl (2.6) von Chiffrierschritten in einem Chiffrierschrittsystem. Gleichgültig, ob ein solches Chiffrierschrittsystem monoalphabetisch oder polyalphabetisch ist: Wenn Unbrechbarkeit skrupulös verlangt wird, sollte ein solcher Chiffrierschritt nie ein zweites Mal verwendet werden.

Im monoalphabetischen Fall muß eine dieser Forderung genügende Chiffrierung polygraphisch sein mit einer Breite, die groß genug ist, um eine ganze Nachricht überdecken zu können. Das wäre eine große praktische Erschwerung, und so wird man eher zu polyalphabetischen Chiffrierungen geringerer Breite, insbesondere zu monographischen, greifen. Überdies kann die skrupulöse Forderung, keinen Chiffrierschritt ein zweites Mal zu verwenden, aufgeweicht werden zu der Forderung eines individuellen Einmal-Schlüssels (8.8), der eine völlige Unregelmäßigkeit der Folge von Chiffrierschritten zeigt, weil dies nach *Kolmogorov* und *Chaitin* bereits Unbrechbarkeit garantiert.

Obschon bereits vor 1930 in den U.S.A., im Deutschen Reich und in der Sowjetunion und auch anderswo individuelle Einmal-Schlüssel für besondere Einsatzgebiete geschätzt wurden, veranlaßten ihre praktischen Nachteile doch dazu, sich weithin mit schwächerer Chiffriersicherheit zufrieden zu geben.

8.9.2 Es kann nicht genügend betont werden, daß (s. 2.6.1) die **Schlüsselvereinbarung** (engl. *key negotiation*) zwischen zwei Partnern eine besondere Schwachstelle jedes kryptologischen Systems ist. Eine sichere Überbrückung einer oftmals großen Entfernung zwischen ihnen hängt (s. unten) an der Zuverlässigkeit der Boten, die zu überwachen selbst schwierig sein kann, und an ihrer Verfügbarkeit.

Es hat deshalb in der Geschichte des Kryptologie nicht an Versuchen gefehlt, die Schlüsselvereinbarung selbst durch kryptologische Maßnahmen zu decken, möglicherweise auch durch Steganographie.

Obschon es verführerisch nahe liegt, die **chiffrierte Schlüsselvereinbarung** für ein kryptologisches System in eben diesem System durchzuführen — insbesondere, wenn man von der Unbrechbarkeit eines solchen felsenfest überzeugt ist —, sollte doch gerade dies vermieden werden, da ein Einbruch in das der Schlüsselvereinbarung dienende Material zur Offenlegung des ganzen Systems führen kann. Zumindest muß, wie es die deutsche Kriegsmarine durch Gebrauch von Bigrammtafeln später tat, die Schlüsselvereinbarung einer zusätzlichen Chiffrierung in einem andersartigen System unterworfen werden.

Die Idee der chiffrierten Schlüsselvereinbarung durch einen **Spruchschlüssel** (engl. *indicator*, s. 19.3.1, 19.6), der die Anfangsstellung eines mechanischen Schlüsselerzeugers beinhaltet, war schon längere Zeit latent und wurde beispielsweise nicht nur für die kommerzielle ENIGMA von 1923 propagiert, sondern auch für die 3-Rotor-ENIGMA der Reichswehr und der Wehrmacht übernommen. Über die Schlüsselvereinbarung erfolgte denn auch prompt

der Einbruch, den (s. 19.6.2, 19.6.4) Marian Rejewski und die anderen jungen polnischen Mathematiker ab 1932 beim deutschen ENIGMA-Verkehr erzielten. Dabei hatten die deutschen Stellen lediglich die Fähigkeiten ihrer Gegner stark unterschätzt und es (mit Ausnahme der Kriegsmarine) nicht für nötig gehalten, das Verfahren der Schlüsselvereinbarung mehr zu komplizieren — immerhin mit der Rechtfertigung, den Nachrichtenverkehr und die Leistungsfähigkeit der Chiffrierer nicht stärker als notwendig zu belasten.

Aufwendigere Verfahren, eine solche angreifbare Schlüsselvereinbarung zu umgehen, sind denkbar, etwa unter Benutzung zweier Chiffrierungen $\mathbf{X}^{(1)}$, $\mathbf{X}^{(2)}$, die vertauschbar sind: $\chi_i^{(1)} \chi_i^{(2)} x = \chi_i^{(2)} \chi_i^{(1)} x$ — zum Beispiel zweier VIGENÈRE- oder VERNAM-Chiffrierungen. Dabei chiffriert der Sender den Klartext zunächst mit $\mathbf{X}^{(1)}$ nach einem von ihm zufällig gewählten Schlüssel $k^{(1)}$, der Empfänger wendet auf das Chiffrat $\mathbf{X}^{(2)}$ an mit einem von ihm zufällig gewählten Schlüssel $k^{(2)}$ und *sendet dieses neue Chiffrat zurück an den Sender.* Dieser faßt es wegen der Vertauschbarkeit von $\mathbf{X}^{(1)}$ und $\mathbf{X}^{(2)}$ als eine von ihm chiffrierte Nachricht auf, die er mit Hilfe seines Schlüssels $k^{(1)}$ dechiffrieren kann. *Das Dechiffrat sendet er an den Empfänger zurück*, der seinerseits sie als eine von ihm chiffrierte Nachricht auffassen kann, die er mit Hilfe seines Schlüssels $k^{(2)}$ dechiffriert und so den Klartext erhält. Nachteilig bei diesem Verfahren ist die Notwendigkeit der dreimaligen Übermittlung. Wenn die Nachricht nur kurz genug ist, könnte das toleriert werden. Die Methode wäre damit gut geeignet für die Übertragung vitaler Information, etwa von Passwörtern oder eines Schlüssels, der nachfolgend für ein anderes Chiffrierverfahren benutzt werden soll. Da jedoch weder Klartext noch einer der Schlüssel offen übertragen werden, scheint das Verfahren sicher zu sein.

Jedoch lauert schon der Reinfall, wie folgendes einfache Beispiel mit zwei VIGENÈRE-Chiffrierungen über $\mathbb{Z}_{26}$ zeigt:

Sender A wählt Schlüssel *A Q S I D*, der dem Empfänger nicht bekannt ist.
Empfänger B wählt Schlüssel *P Z H A F*, der dem Sender nicht bekannt ist.

Der Klartext /image/ wird vom Sender mit *A Q S I D* chiffriert:	i m a g e + *A Q S I D* I C S O H
I C S O H wird dem Empfänger gesandt, der es mit *P Z H A F* chiffriert:	I C S O H + *P Z H A F* X B Z O M
X B Z O M wird dem Sender zurückgesandt, der es mit Hilfe von *A Q S I D* dechiffriert:	X B Z O M − *A Q S I D* X L H G J
X L H G J wird schließlich dem Empfänger zurückgesandt, der es mit Hilfe von *P Z H A F* dechiffriert:	X L H G J − *P Z H A F* i m a g e
und damit die Nachricht /image/ erhält.	

Auf der offenen Übertragungsstrecke befinden sich X B Z O M und I C S O H, deren Differenz jedoch den Schlüssel von B exponiert: (ebenso exponieren X B Z O M und X L H G J den von A).

X B Z O M
− I C S O H
P Z H A F

Damit wird aber auch durch Dechiffrieren von X L H G J mit Hilfe dieses Schlüssels *P Z H A F* der Klartext /image/ bloßgestellt:

X L H G J
− *P Z H A F*
i m a g e

Der Grund für die Einbruchsmöglichkeit liegt darin, daß die Schlüssel bezüglich der Zusammensetzung von Chiffrierungen eine Gruppe bilden (s. 9.1) und noch dazu eine für das Chiffrierverfahren typische — die zyklische Gruppe der Ordnung 26. Die Chiffrierschritte können als bekannt vorausgesetzt werden.

Eine Sicherung gegen den Einbruch besteht nur, wenn mindestens einer der beiden Dechiffriervorgänge so erschwert wird, daß er für den Unbefugten praktisch nicht durchführbar wird. Das bedeutet etwa, ein Chiffrierverfahren zu suchen, bei dem aus der Kenntnis des Schlüssels für die Chiffrierung mit vertretbarem Aufwand nicht der Schlüssel für die Dechiffrierung erzielt werden kann. Wie erst Ende 1997 von der *Communication-Electronics Security Group* des britischen *Government Communications Headquarters* (G.C.H.Q.) offengelegt wurde, stellte eine solche Überlegung 1970 *James H. Ellis* an, und der in der Zahlentheorie bewanderte *Clifford Cocks* fand 1973 in der Multiplikation von hinreichend großen Primzahlen die gesuchte praktisch unumkehrbare Operation. Dann aber kann der Empfänger B sogar öffentlich einen Schlüssel bekanntgeben, mit dem Nachrichten chiffriert werden sollen, die B dechiffrieren kann, und der erste und zweite Schritt des Verfahrens erledigt sich. Es ergibt sich also fast von selbst die Idee eines asymmetrischen Chiffrierverfahrens, die 1976 erstmals publiziert wurde von *Whitfield Diffie* und *Martin E. Hellman* — s. 10.1.2 . Die Briten waren gezwungen, Stillschweigen zu bewahren und mußten mit ansehen, wie ihre Entdeckungen drei Jahre später nochmals gemacht wurden. *James H. Ellis* starb im November 1997.

8.9.3 Sobald ein Nachrichtennetz eine große Anzahl von Knoten und Verbindungen einschließt, muß die gedeckte Schlüsselvereinbarung zu einer **Schlüsselverwaltung** (engl. *key administration, key management*) ausgebaut werden. Die sichere Verteilung von Schlüsseln ist das überragende Problem. Es muß verhindert werden, daß Schlüsselunterlagen auf Transportwegen abgefangen werden können – dazu dient klassischerweise die Übermittlung durch Kuriere (von Diplomaten und Militärs bevorzugt) oder, weniger anspruchsvoll, durch eingeschriebenen Brief (vormals für den privaten Gebrauch oft bevorzugt). Telefon und Telegraf bieten nur zweifelhafte Sicherheit und sind für große Nachrichtenströme sowohl zu langsam wie zu teuer. Offene Systeme wie Internet fallen unter Sicherheitsaspekten völlig aus. Zu einem guten modernen Kryptosystem gehören eingriffsresistente (engl. *tamper-proof*) Schlüsselträger ebenso wie Notfall-Löschungsvorkehrungen. Die Qualitätskontrolle ist bei einem Schlüsselverwaltungssystem ein Gebot.

Ferner bietet die sichere Registrierung und Zuteilung von Schlüsseln ein Problem, dem man mit einem speziellen Benennungssystem steganographisch beizukommen versucht.

Häufig führt man, meist mit praktischen Gründen motiviert, Schlüsselhierarchien mit verschiedenen Sicherheitsebenen ein, etwa für eine Chiffriermaschine mit einem primären, in der Maschine erzeugten Schlüssel, deren Schlüsselerzeuger in gegnerische Hände fallen kann, einen sekundären Schlüssel, der nur für einen relativ kurzen Spruch – sagen wir von einer Länge, die 250 Zeichen nicht überschreitet – gilt, dessen Übermittlung aber nicht sehr hoch gesichert sein muß, und einen hochgesicherten tertiären Schlüssel, der für längere Zeit – sagen wir einen Tag – gilt.[16] Dafür bietet sich nach dem derzeitigen Stand beispielsweise Chiffrierung mit einem Verfahren an, das auf der Widerspenstigkeit (‘*intractability*’) der Berechnung des diskreten Logarithmus (10.2.4.2) beruht. Der mit einer Schlüssellänge von 1024 Bit arbeitende *Key Exchange Algorithm* (KEA) der N.S.A. wurde im Juni 1998 vom U.S. Department of Defense freigegeben.

Solche hierarchischen Systeme machen die Schlüsselverwaltung noch komplexer. Überdies enthalten sie das Risiko des gestuften Angriffswegs: Aufdeckung des Schlüsselerzeugers, Aufdeckung des sekundären Schlüssels, Aufdeckung des gesamten Kryptosystems. Besonders gefährlich ist es, wenn die Vereinbarung über den sekundären Schlüssel mit der Chiffriermaschine selbst chiffriert wird: Ein einmaliger Einbruch kann dann zu einem fortgesetzten Einbruch führen. Der Indikator sollte wenigstens durch ein unabhängiges Chiffrierverfahren gedeckt sein.

Alle Maximen der Schlüsselverwaltung gelten auch für individuelle Einmal-Schlüssel, für die aber auf grund von *Chaitin*s Definition gilt, daß der Schlüssel mindestens so lang ist wie die Nachricht. Durch diesen hohen Schlüsselverbrauch verbietet sich ihr Einsatz in vielen praktischen Fällen, sie wurden mehr und mehr durch quasi-nichtperiodische (Pseudo-Zufalls-)Schlüssel mit bestätigter Qualität verdrängt, insbesondere durch Schlüssel, deren überaus lange Periode garantiert werden kann und die hinreichend viele statistische Tests bestanden haben. Häufig werden dabei umfängliche zahlentheoretische Untersuchungen erforderlich. Jedoch könnte der Fortschritt in den Speichertechnologien manche Nachteile, die die Verbreitung von individuellen Einmal-Schlüsseln in großen Massen mit sich bringt, mildern. Leichtgewichtige Speicherscheiben (CD-ROM) mit einer Dichte von einigen Gigabytes per Dekagramm geben individuellen Einmal-Schlüsseln eine neue Chance, in hochgesicherten diplomatischen, strategischen und kommerziellen Nachrichtenwegen mit garantierter absoluter Unbrechbarkeit eingesetzt zu werden.

---

[16] Für das Beispiel der Wehrmachts-ENIGMA nach der vom 8. Juli 1937 bis 15. September 1938 gültigen Vorschrift: Als sekundärer Schlüssel diente ein ‚Spruchschlüssel‘, ein Indikator zur Anfangseinstellung der Rotoren für den einzelnen Spruch; als tertiärer Schlüssel diente ein ‚Tagesschlüssel‘, der (Abb. 51) Walzenlage, Ringstellung, Grundstellung und Steckerverbindungen enthielt. Das primäre und das sekundäre Chiffriersystem waren jedoch identisch, der tertiäre Schlüssel wurde durch Kurier übermittelt.

9 Komposition von Chiffrierverfahren

Es sei zunächst daran erinnert, daß eine Chiffrierung $\mathbf{X} : V^* \dashrightarrow W^*$ gewöhnlich endlich erzeugt wird durch Chiffrierschritte aus einem **Chiffrierschritt-System** M. M^* bezeichnet die Menge aller Chiffrierungen, die auf diese Weise durch M erzeugt werden. Eine **Chiffriermethode** S ist eine Teilmenge von M^*. M^d bezeichnet die Teilmenge aller Chiffrierungen mit Schlüsselfolgen der Periode d, M^∞ die Teilmenge aller Chiffrierungen mit nicht-berechenbaren Schlüsselfolgen.

Eine Komposition zweier Chiffrierschritt-Systeme durch Hintereinanderausführung ihrer Chiffrierungen verlangt, daß der Bildbereich der ersten im Argumentbereich der zweiten liegt.

Der Laie neigt dazu, zu glauben, eine Komposition zweier Chiffrierschritt-Systeme biete der unbefugten Entzifferung mehr Widerstand als jedes der beiden einzeln. Das kann so, muß aber nicht so sein. Das zweite Chiffrierschritt-System kann ja sogar die Wirkung des ersten teilweise oder ganz aufheben. So sei S eine einfache Substitution, die, wie üblich, durch einen Merkvers erzeugt wird, etwa dem folgenden (der von *Bazeries* stammen könnte):

BASEDOWSCHE KRANKHEIT .

Die Substitution lautet dann

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	A	S	E	D	O	W	C	H	K	R	N	I	T	F	G	J	L	M	P	Q	U	V	X	Y	Z

Zweimal angewandt ergibt sie

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	B	M	D	E	F	V	S	C	R	L	T	H	P	O	W	K	N	I	G	J	Q	U	X	Y	Z

wobei neun Buchstaben, darunter die häufigen Vokale e a o , invariant sind.

9.1 Gruppeneigenschaft

Einige Klassen endomorpher Chiffrierungen, bei denen $V \equiv W$ ist, haben die Eigenschaft, daß die Komposition zweier Chiffrierungen nicht aus der Verfahrensklasse hinausführt. Man sagt, eine solche Chiffrierung bildet eine **Gruppe**: Beispiele sind die Gruppe $\mathcal{P}_{26}$ aller einfachen Permutationen über Z_{26}, die Gruppe $\mathcal{P}_{24}$ aller Transpositionen der Breite 24.

Für andere Chiffrierungen ist das nicht notwendigerweise so: Eine Menge von voll zyklischen einfachen Substitutionen bildet keine Gruppe, da die Gruppenidentität nicht voll zyklisch ist. Die Beispiele in 7.2.4 zeigen, daß die Menge der ALBERTI-Chiffrierschritte und die Menge der ROTOR-Chiffrierschritte für gewisse Referenzalphabete keine Gruppe bilden. Die Komposition solcher Schritte erhöht die kombinatorische Komplexität. Solche Kompositionen werden in Chiffriermaschinen benutzt. Die ENIGMA und ihre Verwandten benutzten eine Komposition von ROTOR-Chiffrierungen zur Vergrößerung der kombinatorische Komplexität. Klassen von Chiffrierungen, die keine Gruppen sind, sind also in einem gewissen Sinn vorteilhaft.

9.1.1 Bildet jedoch ein Chiffrierschritt-System eine Gruppe, so ist die Menge der Chiffrierschritte gegen Zusammensetzung **abgeschlossen**: Die Zusammensetzung zweier Chiffrierschritte $\chi_s \in M$, $\chi_t \in M$ gehört wieder der Menge M an: $\chi_s(\chi_t(p)) = \chi_{s\bullet t}(p)$, wodurch $s \bullet t$ eindeutig definiert ist. Die Schlüssel bilden also eine Gruppe, die **Schlüsselgruppe** (engl. *key space*). Eine Chiffrierung mit einer Schlüsselgruppe hat *Shannon* '*pure cipher*' genannt.

9.1.2 Auch eine Chiffriermethode kann eine Gruppe sein im Hinblick auf die Komposition ihrer Chiffrierungen: die Gruppe aller linearen Substitutionen mit einer gewissen Breite n, die Gruppe aller polyalphabetischen (monographischen) Substitutionen mit einer gewissen Periode d, die Gruppe aller Block-Transpositionen mit einer gewissen Breite n.

Die Komposition zweier Chiffriermethoden führt jedoch im allgemeinen zu einer neuen, obschon meist verwandten Chiffriermethode: Die Komposition zweier linearer polyalphabetischer oder zweier allgemeiner polyalphabetischer Chiffriermethoden mit den jeweiligen Perioden d_1 und d_2 ist eine lineare bzw. allgemeine polyalphabetische Chiffrierung, mit der Periode $kgv(d_1, d_2)$. Entsprechendes gilt für zwei Blocktranspositionen der Breite n_1 und n_2. Für lineare Substitutionen wußte das schon *Babbage* 1854.

Kompositionen von zwei oder mehreren gänzlich verschiedenen Chiffriermethoden („Produktchiffrierung") kommen häufig vor. Manche solcher Kompositionen sind vertauschbar, wie die Gruppe aller einfachen Substitutionen mit der Gruppe der Transpositionen der Breite n. In diesem Fall bildet die kombinierte Chiffriermethode wieder eine Gruppe (*Shannon*: *The product of two pure ciphers which commute is pure*).

9.1.3 Hierunter fällt die im SIEMENS Chiffrier-Fernschreiber (s. 8.7.3) über $\mathbb{Z}_2^5$ vorliegende Komposition einer Pentagramm-Substitution (VERNAM-Chiffrierschritte angewandt auf 5-Bit-Codegruppen) mit einer 5-Bit-Codegruppen-Transposition (Permutation der fünf Plätze), in gruppentheoretischer Sprechweise eine Untermenge der Hyperoktaedergruppe im $\mathbb{R}_5$, die von der Ordnung $2^5 \cdot 5! = 3840$ ist. Die SIEMENS Chiffrier-Fernschreiber beruhten auf einem deutschen Patent, das *August Jipp* und *Ehrhard Rossberg* am 18. Juli 1930 eingereicht hatten.

Die Modelle T 52a und T 52b[1] wurden von der Kriegsmarine ab 1931 im Küstenverkehr für Drahtverbindungen benutzt. Das Modell T 52c wurde zuerst hauptsächlich von der Luftwaffe eingesetzt, ab Mitte 1941 allgemein von der Wehrmacht (‚Geheimschreiber'), britischer Deckname STURGEON (Stör). Von diesen und späteren Modellen wurden über die Jahre schätzungsweise 1 000 Stück gebaut.

Zur Chiffrierung und Dechiffrierung wurden 10 Stiftwalzen w_s benützt, die binäre Schalter (‚Umschalter') i_s betätigten mit $i_s = 0$ oder $i_s = 1$, $s = 1 ... 10$. Die ersten fünf der Stiftwalzen $w_1 ... w_5$ arbeiteten dabei mit VERNAM-Schritten auf die einzelnen Bits der Fünfergruppen des Fernschreibalphabets und bewirkten *eine* von 32 involutorischen Substitutionen, die anderen fünf Walzen $w_6 ... w_{10}$ erzielten eine von höchstens 32, tatsächlich von 30, im allgemeinen nicht-involutorischen Transpositionen der Bits der Fünfergruppe. Im Modell T 52a war das die Menge $\{(12)^{i_1}(23)^{i_2}(34)^{i_3}(45)^{i_4}(51)^{i_5} : i_s \in \{0,1\}\}$, wegen $(12)(23)(34)(45) = (54321)$, $(23)(34)(45)(51) = (54321)$ und $(23)(34)(45) = (5432)$, $(12)(23)(34)(45)(51) = (5432)$ beträgt die Anzahl *verschiedener* Transpositionen nur 30 (ein Viertel der $5! = 120$ möglichen *Permutationen*). Insgesamt erzeugten die 10 Stiftwalzen also 960 Alphabete, ein Viertel der 3840 Decktransformationen der Hyperoktaedergruppe.

Im T 52c, der von *Herbert Wüsteney* (1899–1988) entwickelt wurde, konnte überdies ein ‚Spruchschlüssel' eingestellt werden. Beim T 52e traten infolge einer konstruktiven Änderung nur 16 verschiedene Substitutionen und 15 verschiedene Transpositionen auf; die Anzahl der in einem Spruch verwendeten Alphabete ging auf 240 zurück. Beim T 52c waren es lediglich 120 Alphabete.

Die Stiftwalzen dienten auch zur Fortschaltung. Zu diesem Zwecke hatten sie der Reihe nach 47, 53, 59, 61, 64, 65, 67, 69, 71 und 73 Zähne, bei jedem Schritt wurden alle Walzen um einen Zahn bewegt, das ergab eine Art regulärer Fortschaltung mit einer Periode von $47 \cdot 53 \cdot 59 \cdot 61 \cdot 64 \cdot 65 \cdot 67 \cdot 69 \cdot 71 \cdot 73$, d.h. knapp 10^{18}.

T 52d und T 52e (eingeführt 1943 und 1944) unterschieden sich von T 52a bzw. T 52c durch Hinzufügen einer besonderen Form unregelmäßiger „aussetzender" Fortschaltung und fakultativ einer ‚Klartextfunktion'. Auf diesen Gedanken ('*influence letter*', schwed. Pat. 52279, U.S. Patent 1 502 376) war bereits in den frühen zwanziger Jahren *Arvid Gerhard Damm* gekommen.

9.1.4 Kryptologisch einfacher ging man in den Chiffrier-Fernschreibern (‚Schlüsselzusatz') SZ 40, SZ 42, SZ 42a, britischer Deckname TUNNY (Thunfisch) von LORENZ vor. Sie führten nur Substitutionen durch, die Chiffrierung war dementsprechend involutorisch. In der SZ 42 (Farbtafel N) wirkte eine erste Gruppe von fünf Stiftwalzen mit den Perioden 41, 31, 29, 26, 23 (von den Briten χ-*wheels* genannt) mit VERNAM-Schritten auf die Bits der Fünfergruppen; jede Walze dieser Walzengruppe wurde für jedes Zeichen um einen Schritt fortgeschaltet. Eine zweite Gruppe von fünf Stiftwalzen mit den

[1] Die T 52b unterschied sich von der T 52a nur durch eine verbesserte Funkentstörung.

Perioden 43, 47, 51, 53, 59 (von den Briten ψ-*wheels* genannt) war der ersten Gruppe nachgeschaltet, wieder mit VERNAM-Schritten. Zwei weitere Walzen (von den Briten *motor-wheels* genannt) dienten nur der unregelmäßigen Fortschaltung: Eine mit der Periode 61, mit der ersten Walzengruppe bewegt, steuerte eine zweite mit der Periode 37; diese wiederum steuerte die *gleichzeitige* Bewegung (eine Schwachstelle!) aller Walzen der zweiten Walzengruppe. Sämtliche Stiftwalzen konnten beliebig mit Stiften versehen werden; sie konnten überdies in jede Ausgangsstellung gebracht werden, erlaubten also die Einstellung eines Spruchschlüssels. Die Periode lag über 10^{19} .

9.1.5 Wenig ist bekannt über den Einsatz eines Chiffrier-Fernschreibers von OLIVETTI (Italienisches Patent 387 482, 30. Januar 1941), der bloß fünf Chiffrierräder und zwei *motor wheels* hatte und nur eine schwache Irregularität der Fortschaltung aufwies.

9.2 Überchiffrierung

9.2.1 Überchiffrierung (engl. *superencryption*, *closing*, auch U.S. *superenciphering*, U.K. *reciphering*, franz. *surchiffrement*), im Jargon auch ‚Überschlüsselung' genannt, ist ein häufiger Fall einer Produktchiffrierung: Ein Buchstaben-Code oder Ziffern-Code wird nochmals chiffriert. Im letzteren Fall wird gerne VIGENÈRE über $\mathbb{Z}_{10}$, d.h. mit $N = 10$, benutzt. Solche Verfahren, die die Addition *modulo* 10 , also ohne Übertrag, bewerkstelligen, wurden im militärischen Bereich gelegentlich ‚symbolische Addition' genannt; sie sind auf einer verstümmelten Addiermaschine leicht durchführbar, vgl. 8.3.3. Bereits 1780 wurde von dem für England spionierenden *Benedict Arnold* die stellenweise Addition von 7, also eine gewöhnliche CAESAR-Addition, als Überchiffrierung benutzt. Wird nicht stellenweise, sondern für Gruppen der Chiffrierbreite n eine Zahl *modulo* 10^n addiert (polygraphische CAESAR-Addition), spricht man von einem **Additiv** (engl. *additive*). Die Verwendung von Additiven wurde schon im 19. Jahrhundert in Verbindung mit dem Erscheinen von Codebüchern bekannt. Zur Erleichterung der Berechnung werden manchmal törichterweise spezielle Additive benutzt, wie 02000 . Dies ist auch noch zu beanstanden in folgendem besonderen Fall von **doppelter Überchiffrierung**: Codebücher, die sowohl Buchstabengruppen wie Zifferngruppen enthalten, erlauben eine an die Addition anschließende Überchiffrierung der Zahlengruppen durch korrespondierende Buchstabengruppen. *J. N. H. Patrick* wurde überführt, 1876 in einer Bestechungsaffäre im U.S. Congress ein solches System benutzt zu haben. Die U.S. Navy verwendete das System im Spanisch-Amerikanischen Krieg 1898; man betrachtete es zu dieser Zeit als das sicherste und fortgeschrittenste System, vorausgesetzt die Additive waren nichttrivial und wurden in kurzen Intervallen gewechselt.

Das Auswärtige Amt des Deutschen Reiches benützte seit 1919 eine doppelte Überchiffrierung eines fünfziffrigen Codebuches („Deutsches Satzbuch", DESAB). Dazu wurden zwei über sechs Fünfergruppen gehende Additive

verwendet. 5000 solcher Additive und ihre jeweiligen Komplemente waren verfügbar. Die Briten versuchten lange Zeit vergeblich einen Einbruch in das System, dem sie die Decknamen GEC oder FLORADORA gaben. Im Mai 1940 erbeuteten sie jedoch im Deutschen Konsulat Reykjavik auf Island Chiffrierunterlagen, darunter zwei Codebücher No. 22, No. 46 und zehn Additive. Das reichte zunächst nur aus zu kleinen Fortschritten durch Probieren auf stereotype Wendungen. Als jedoch 1942 dem britischen Konsul in Lourenço Marques, der Hauptstadt des portugiesischen Moçambique, durch einen glücklichen Zufall die Additive für die nächsten zwei Monate in die Hände fielen, gelang Alastair G. Denniston, F. W. ('Bill') Filby und dem reaktivierten Ernst C. Fetterlein in Bletchley Park in Zusammenarbeit mit Solomon Kullback in Washington schließlich 1944 ein vollständiger Einbruch.

Transposition mag ebenfalls zur Überchiffrierung genutzt werden: *F. J. Sittler*, einer der erfolgreichsten Codebuchfabrikanten, empfahl, die vier Ziffern seines Codes zu permutieren. Bei festgehaltener Permutation entsteht dabei (wie bei festgehaltenem Additiv) lediglich ein neuer Code, nicht sicherer als der alte. Wenn schon eine Transposition benutzt wird, sollte ihre Breite relativ prim zur Codelänge sein.

9.2.2 Überchiffrierung ist insbesondere angezeigt für Angaben wie Daten, Uhrzeiten, Namen, Koordinaten usw., die besonders sicherheitsbedürftig sind. Auch polygraphische Substitutionsverfahren können genutzt werden, ein Beispiel lieferte die Überchiffrierung eines taktischen 3-Ziffern-Codes (‚Schlüsselheft', im 1. Weltkrieg ab März 1918 von der deutschen Truppe an der Westfront benutzt) mit einer bipartiten Bigrammsubstitution (4.1.2, Abb. 32 ‚Geheimklappe'). Ein weiteres Beispiel lieferte die ENIGMA-Überchiffrierung codierter Netzkoordinaten (2.5.3) bei der deutschen Kriegsmarine im 2. Weltkrieg.

9.2.3 Eine feste Überchiffrierung der ENIGMA-Chiffrierung durch eine Substitution (3.2.4) brachte das Steckerbrett zustande. Die Substitution hätte nicht involutorisch sein müssen, eine beliebige Substitution hätte den involutorischen Charakter der ENIGMA erhalten. Die gegen die Überchiffrierung durch das Steckerbrett unempfindlichen kryptanalytischen Methoden, die die Polen und die Briten anwendeten (Zygalski-Lochblätter, Turing-Bombe), wären allerdings auch bei einer beliebigen Substitution wirksam geblieben. Hingegen hätte *Welchman*s 'diagonal board' nichts mehr genützt.

9.2.4 Ein elementarer Fall einer gründlichen Durchmischung liegt vor bei dem von Leutnant *Fritz Nebel* (1891–1967) erfundenen ADFGVX-System des kaiserlichen Heeres von 1918 vor, einer 6×6-Polybius-Substitution (3.3.1) in das Alphabet {A, D, F, G, V, X} (vgl. 2.5.2) von Morsezeichen, gefolgt von einer Transposition der Breite 20. Das Verfahren wurde 1918 unter *Ludendorff* an der Westfront eingesetzt. Bei täglich wechselndem Schlüssel kostete es den französischen Kryptologen *Painvin* oft mehrere Tage, bestenfalls jedoch nur einen Tag, bis er den Funkspruch entziffert hatte.

9.2.5 Im ENIGMA-Funkverkehr der Kriegsmarine wurden Nachrichten von besonderer Tragweite nochmals in besonderer Weise überchiffriert, kenntlich gemacht durch die Kenngruppe (engl. *discriminant*) OFFIZIER. Grund dafür war auch die Abschirmung vor der Mannschaft. Am späten Abend des 20. Juli 1944 ging ein Rundspruch an die Schiffe, den die Briten entzifferten:

OKMMMANANALLEXXEINSATZJWALKUEREJNURDURCHOFFIZIERZUENTZIFFERN
OFFIZIERJDORAJDERFUEHRERJADOLFHITLERJISTTOTXDERNEUEFUEHRERIS
TFELDMARSCHALLJVONWITZLEBENJ ......

Walter Eytan [Ettinghausen], Wachhabender in *Bletchley Park*, der nicht wissen konnte, wie makaber der falsche Teil der Nachricht war, hielt sie jedenfalls vor den dort arbeitenden Hilfskräften, den *wrens* ('Women's Royal Naval Section') geheim – sicher ist sicher.

9.3 Ähnlichkeit von Chiffrierverfahren

Claude Shannon nennt zwei Verfahrensklassen $\mathcal{T}$, $\mathcal{S}$ ähnlich, wenn es eine (vom Schlüssel unabhängige) eineindeutige Abbildung A des Bildbereichs von $T \in \mathcal{T}$ in den Bildbereich von $S \in \mathcal{S}$ gibt, derart daß

$$\forall\, T \in \mathcal{T} \;\; \exists\, S \in \mathcal{S} : \;\; S = AT \;, \quad \text{d.h.} \quad S(x) = AT(x) \;\; \text{für alle } x\,.$$

Ähnliche Verfahrensklassen sind kryptanalytisch gleichwertig: Man darf annehmen, daß A bekannt ist (*Kerckhoffs*' Maxime in der Fassung von *Shannon*: *"The enemy knows the system being used"*). Jede Möglichkeit, T zu brechen, ist dann auch eine Möglichkeit, S zu brechen. Ähnlich sind:

CAESAR-Verfahren und revertiertes CAESAR-Verfahren
(A ist die Revertierung des Bild-Alphabets),

VIGENÈRE-Verfahren und BEAUFORT-Verfahren
(A ist die Revertierung des Bild-Alphabets),

einfache Spaltentransposition und Blocktransposition
(A ist die Matrix-Transposition).

9.4 Durchmischung nach Shannon

Nicht vertauschbar sind eine multipartite monographische Substitution und eine Transposition. Nicht vertauschbar ist auch die Komposition einer echt polygraphischen Substitution der Breite k mit einer Transposition der selben Breite k. Nicht vertauschbar sind ferner VIGENÈRE-Schritte und einfache Substitutionen (zusammen ergeben sie die in 7.2.1 mit dem Stichwort ALBERTI-Schritte bezeichnete Familie)[2]. Die Komposition nicht-vertauschbarer Verfahren gibt eine gute Ausgangsbasis für eine gründliche ‚Durchmischung', wie sie *Shannon* empfahl. Er verglich sie mit der Herstellung

---

[2] *Eyraud* bespricht auch die Komposition: einfache Substitution-VIGENÈRE-einfache Substitution, die er ≪alphabets non-normalement parallèles≫ nennt (s. 8.2.3).

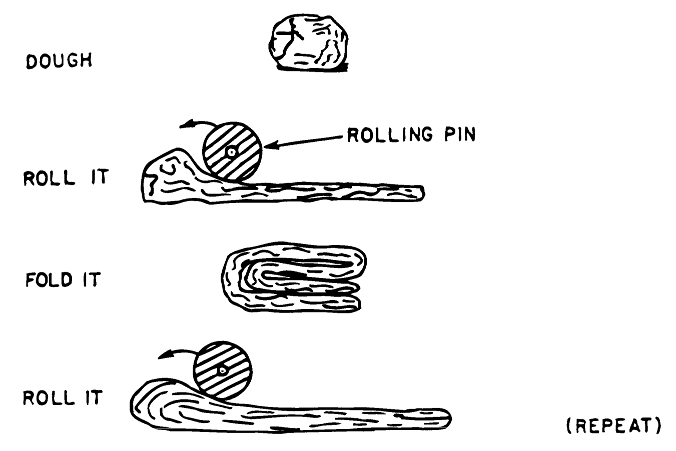


Abb. 71. Herstellung von Blätterteig
(Aus: *N. J. A. Sloane*, Encrypting by Random Rotations. L. N. C. S. **149**, S. 75)

von Blätterteig durch wiederholte Anwendung von Ausrollen und Falten (Abb. 70), ein von *Eberhard Hopf*[3] studiertes Beispiel für Transformationen kompakter Räume.

9.4.1 Gefühlsmäßig wird man eine Komposition besonders wirkungsvoll finden, wenn die kombinierten Verfahren nicht nur nicht kommutieren, sondern auch möglichst ‚windschief' zueinander liegen, wie Transposition, die nach *Shannon* eine ‚Diffusion' bewirkt und lineare polygraphische Substitution, die eine ‚Konfusion' bewirkt. Ist diese Komposition keine Gruppe, so sollte eine wiederholte Anwendung eine besonders gründliche **Durchmischung** herbeiführen. In diskreten Räumen ist jedoch jede **Iteration** einer festen Transformation schließlich periodisch und die Shannon-Hopfsche Durchmischung unterliegt der Gefahr einer Selbsttäuschung, wie das nachfolgende Beispiel (Abb. 72a und Abb. 72b) einer iterierten ‚Bildtransformation' zeigt, die zunächst in überzeugender Weise für eine Durchmischung sorgt.



Abb. 72a. Modulare Transformation

[3] *Eberhard Hopf*, On Causality, Statistics and Probability, Journal of Math. and Physics **13**, 51–102, 1934.

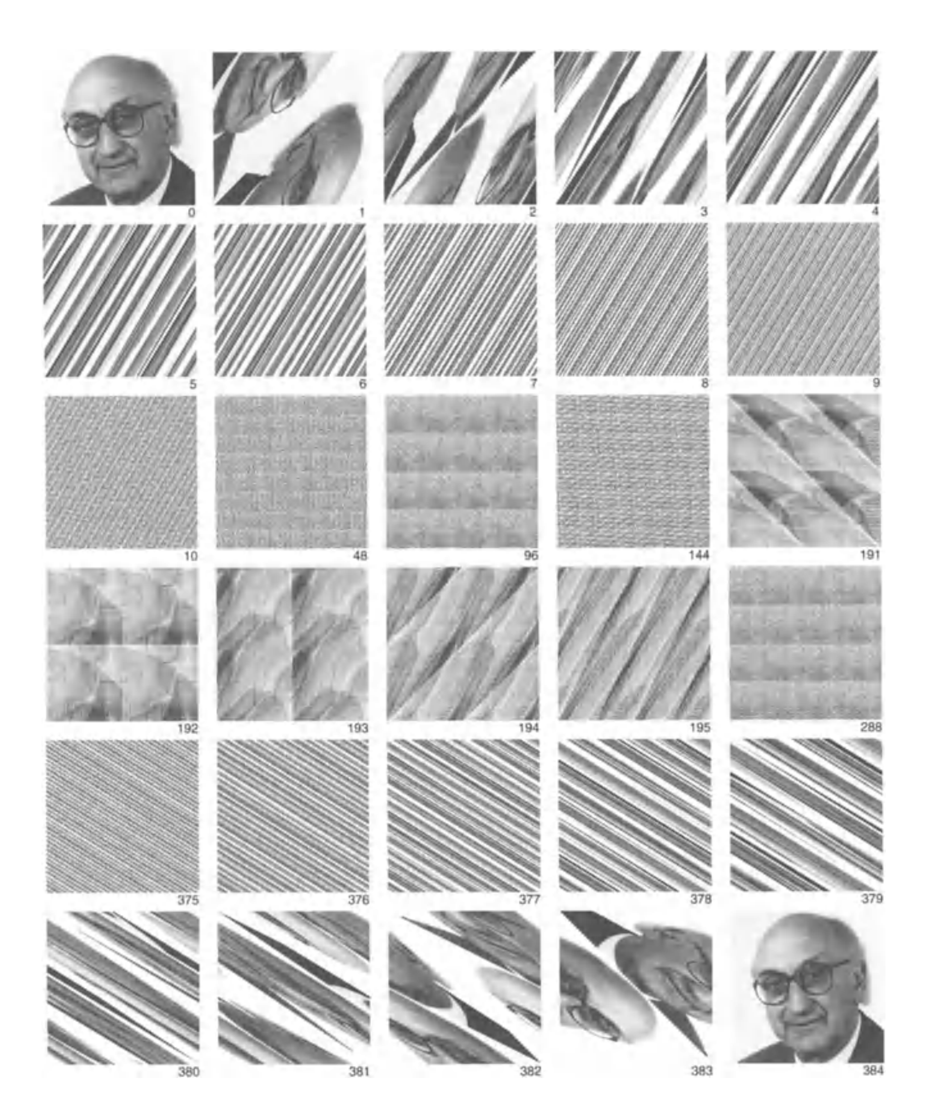
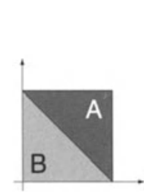


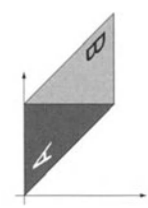
Abb. 72b. *FLB*s Auferstehung

Der Transformationsschritt besteht aus einer Spiegelung mit affiner Verzerrung, gefolgt von einer Reduktion auf das Bildformat durch Abschneiden und Ankleben überstehender Ecken (Abb. 72a). Das Ergebnis sukzessiver Transformationsschritte zeigt Abb. 72b. Zunächst sieht es aus, als ob der abgebildete *FLB* durchmischt würde, aber nach 48 Schritten zeigt sich eine Textur und nach 192 Schritten tritt er schemenhaft 4-fach auf; nach 384 Schritten schließlich kommt gar das ursprüngliche Bild wieder. Eine Bildchiffrierung der angegebenen Art mit einer hohen Iterationszahl trägt also die Gefahr in sich, nichts zu verbergen.

9.4.2 Wie ist das Phänomen zu erklären? Wir betrachten das Quadrat $Q: \ 0 \le x < 1 \ , \ 0 \le y < 1$ mit torusförmigem Zusammenhang und darauf die modulare Transformation (Abb. 73)

$$T: \begin{cases} x' = y \\ y' = \begin{cases} x+y-1 & \text{falls} \quad x+y \ge 1 \\ x+y & \text{falls} \quad 0 \le x+y < 1 \end{cases} \end{cases}$$





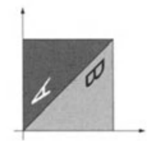
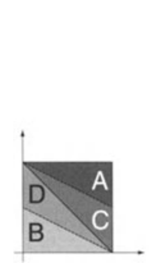
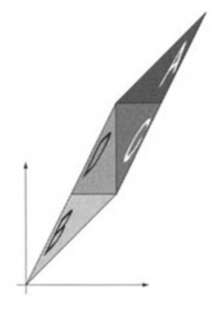


Abb. 73. Modulare Transformation T

Die lokale Affinverzerrung samt Spiegelung T wird durch die Matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ bewerkstelligt[4] , die schon in 8.6.1 aufgetreten ist.





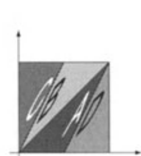


Abb. 74. Modulare Transformation T^2

Abb. 74 zeigt die Wirkung von T^2 mit der durch die Matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

bewirkten lokalen Affinverzerrung, Abb. 75 schließlich die von T^4 mit

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^4 = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} + 3 \cdot \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} .$$

---

[4] Es ist $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}$, wo F_i die i-te Fibonaccizahl ist. Siehe auch *F. L. Bauer*, Efficient Solution of a Non-Monotonic Inverse Problem. In: *W. H. J. Feijen et al.* (eds.), Beauty is our Business. Springer, New York 1990, S. 19–26 .

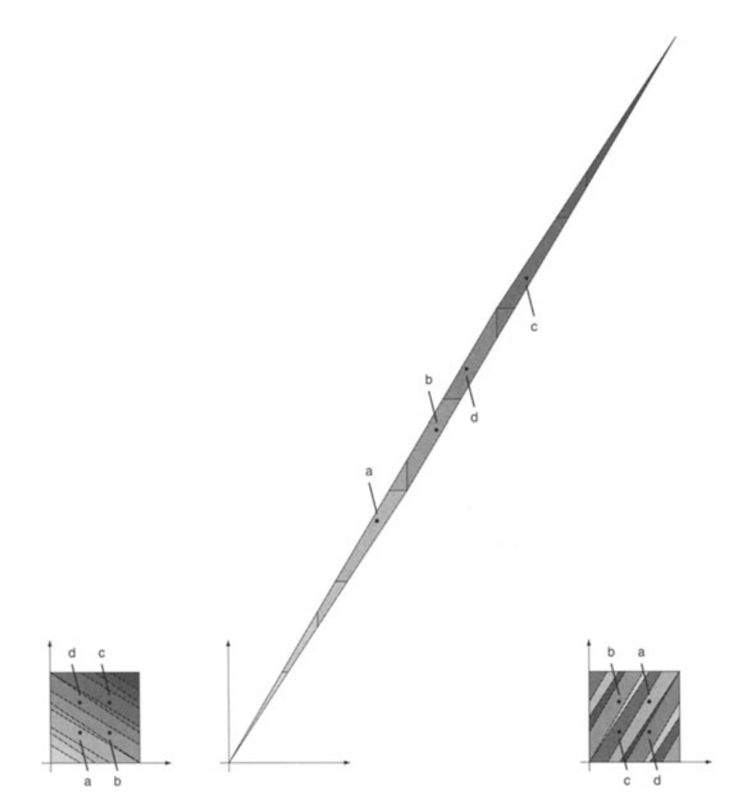


Abb. 75. Modulare Transformation T^4

Hier tritt bereits das Phänomen auf, daß die Figur der vier Punkte

$$a = \begin{pmatrix} \frac{1}{3} \\ \frac{1}{3} \end{pmatrix}, \quad b = \begin{pmatrix} \frac{2}{3} \\ \frac{1}{3} \end{pmatrix}, \quad c = \begin{pmatrix} \frac{2}{3} \\ \frac{2}{3} \end{pmatrix}, \quad d = \begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \end{pmatrix}$$

um 180° gedreht wird. Entsprechend sind unter T^8 mit der Matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^8 = \begin{pmatrix} 13 & 21 \\ 21 & 34 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 3 \cdot \begin{pmatrix} 4 & 7 \\ 7 & 11 \end{pmatrix}$$

diese vier Punkte bereits Fixpunkte. Für T^{16} mit der Matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{16} = \begin{pmatrix} 610 & 987 \\ 987 & 1597 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 21 \cdot \begin{pmatrix} 29 & 47 \\ 47 & 76 \end{pmatrix}$$

kommen weitere Fixpunkte hinzu, tatsächlich gilt

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{16} \begin{pmatrix} \frac{i}{21} \\ \frac{k}{21} \end{pmatrix} = \begin{pmatrix} \frac{i}{21} \\ \frac{k}{21} \end{pmatrix} + \begin{pmatrix} 29\,i + 47\,k \\ 47\,i + 76\,k \end{pmatrix}.$$

Es sind also alle 400 Punkte mit den Koordinaten $\frac{i}{21}$, $\frac{k}{21}$ $(0 < i,\ k < 21)$ Fixpunkte. Zu T^{48} gehört die Matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{48} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 46\,368 \cdot \begin{pmatrix} 64\,079 & 103\,682 \\ 103\,682 & 167761 \end{pmatrix}, \text{ wobei}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{48} \begin{pmatrix} \frac{i}{46368} \\ \frac{k}{46368} \end{pmatrix} = \begin{pmatrix} \frac{i}{46368} \\ \frac{k}{46368} \end{pmatrix} + \begin{pmatrix} 64079\,i + 103682\,k \\ 103682\,i + 167761\,k \end{pmatrix} \quad (0 < i,\, k < 46368).$$

Das ergibt $46367^2 = 199^2 \cdot 233^2 \approx 2.15 \cdot 10^9$ Fixpunkte. *Außerhalb* dieser Punkte tritt jedoch eine starke Durchmischung ein.

Wird allerdings durch Rasterung die Bildschwärzung beschränkt auf ein Gitter, so ist die Wiederherstellung des Bildes nach hinreichend vielen Iterationen verständlich, wenn die Fixpunktmenge die Menge der Rasterpunkte umfaßt: Beachte daß $46368 = 2^5 \cdot 3^2 \cdot 7 \cdot 23$. Somit

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{48} \bmod 2^5 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Das bedeutet, daß im Beispiel von Abb. 72 bei einem Raster von 32×32 Gitterpunkten nach 48 Schritten die Auferstehung geschehen müßte. Tatsächlich wurde die Rasterung mit 256×256 Gitterpunkten durchgeführt, somit

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{48} \bmod 2^8 = \begin{pmatrix} 2\,971\,215\,073 & 4\,807\,526\,976 \\ 4\,807\,526\,976 & 7\,778\,742\,049 \end{pmatrix} \bmod 2^8 = \begin{pmatrix} 225 & 64 \\ 64 & 33 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{96} \bmod 2^8 = \begin{pmatrix} 225 & 64 \\ 64 & 33 \end{pmatrix}^2 \bmod 2^8 = \begin{pmatrix} 193 & 128 \\ 128 & 65 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{192} \bmod 2^8 = \begin{pmatrix} 193 & 128 \\ 128 & 65 \end{pmatrix}^2 \bmod 2^8 = \begin{pmatrix} 129 & 0 \\ 0 & 129 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{384} \bmod 2^8 = \begin{pmatrix} 129 & 0 \\ 0 & 129 \end{pmatrix}^2 \bmod 2^8 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Daher das Resultat, das die Tabelle in 8.6.1 erweitert: $r(T, 256) = 384$.

Das gewählte Beispiel einer Bildchiffrierung ließe sich natürlich auch auf Textchiffrierung durch Transposition übertragen.

9.4.3 Allgemein soll man nach *Shannon* Kompositionen $\mathcal{S}\,\mathrm{F}\,\mathcal{T}$ in Betracht ziehen, wo $\mathcal{S}$ und $\mathcal{T}$ vergleichsweise einfache Verfahrensklassen und F eine (feste) Transformation ist, die eine gründliche Durchmischung bringt. Im Beispiel der tomographischen Verfahren (4.2) wäre das die zwischengeschaltete Transposition, im Beispiel der gemischten Zeilen-Spalten-Transposition (6.2.3) wäre es die zwischengeschaltete Matrix-Transposition. In modernen Anwendungen könnte es ein Chip sein, der eine Familie von 64 Bit breiten polygraphischen Substitutionen festlegt. Von ungezügeltem Zutrauen in die Wirksamkeit solcher ‚Barrieren', wie *Shannon* sie nennt, muß jedoch gewarnt werden; es besteht immer die Gefahr einer *complication illusoire*. Im übrigen bringt die vollständige Durchmischung auch einen großen praktischen Nachteil mit sich: Ein einzelner Chiffrierfehler kann, ja muß sich über die ganze entzifferte Nachricht ausbreiten (‚Lawineneffekt', s. 11.3 (5)) und macht diese nicht nur lokal, sondern global unleserlich, mit allen Konsequenzen bei eventueller Wiederholung (s. 11.1.1). Die Durchmischung des Blätterteigs ist in diesem Fall gefährlich gut.

9.4.4 Eine einfache, praktisch brauchbare und sehr starke Durchmischung bewirken die **tomographischen Verfahren**: Nach einer multipartiten Substitution wirkt als Barriere eine spezielle Transposition; die Bestandteile werden ,zerschnitten' und anders zusammengefügt, zum Schluß wird eine multigraphische Rücksubstitution vorgenommen.

Die Idee scheint als erster *Honoré Gabriel Riqueti Comte de Mirabeau* (1749–1791), frz. Publizist und Politiker, gehabt zu haben. Nach einer bipartiten, eineindeutigen Polybius-Substitution (vgl. 3.3.1) $\mathbb{Z}_{25} \longrightarrow \mathbb{Z}_5 \times \mathbb{Z}_5$ gruppierte er zunächst alle ersten Ziffern, dann alle zweiten Ziffern zusammen und wandte die umgekehrte Polybius-Substitution $\mathbb{Z}_5 \times \mathbb{Z}_5 \longrightarrow \mathbb{Z}_{25}$ an. Daran schloß sich vermutlich ein steganographisches Verfahren an – *Bazeries*, der angibt, einige authentische Briefe der *Marquise Sophie de Monnier* an ihren berühmten Liebhaber entziffert zu haben, wobei er den ≪*teneur pornographique*≫ erwähnt, gibt keine weiteren Einzelheiten, stellt aber die Bemerkung in den Zusammenhang mit *Boetzel* und *O'Keenan* (vgl. 1.2).

Mit der Hin- und Zurückchiffrierung $\mathbb{Z}_{25} \longleftrightarrow \mathbb{Z}_5 \times \mathbb{Z}_5$ (Anarchistenchiffre) beschäftigte sich schon *Lewis Carroll* (Tagebuchnotiz vom 26. Februar 1858).

9.4.5 Die Polybius-Substitution kommt in anderer Weise auch in den frühen Chiffriermaschinen B-21, B-211 von *Boris Hagelin* vor. *Hagelin* verwendete zwei *Damm*sche Halbrotoren mit zehn Stellungen, um für jede der beiden $\mathbb{Z}_5$ zehn verschiedene Alphabete (zweimal fünf verschobene) zu erhalten; insgesamt wurden also damit 100 verschiedene Alphabete erzielt. Die Fortschaltung geschah durch zwei mal zwei Schlüsselräder mit den Teilungen 17, 19, 21 und 23. Die B-211 besaß zusätzlich ein Steckerfeld.

Die von *Alexis Koehl* 1876 vorgeschlagene tomographische Methode beruhte nach *Gyldén* auf einer multipartiten Substitution $\mathbb{Z}_{25} \longrightarrow \mathbb{Z}_{10} \times \mathbb{Z}_{10}$.

9.4.6 *Delastelle*[5] diskutierte auch eine tomographische Methode, die nach der Zerschneidung einer bipartiten Chiffre statt der von *Mirabeau* benutzten lokalen Umgruppierung eine allgemeinere anwendet, ferner Rückübersetzung mittels der gleichen oder einer **konjugierten** Chiffre. Für die Umgruppierung schlug er eine *longueur de sériation* vor, beispielsweise 7 in folgendem Beispiel mit der aus BORDEAUX (4.2.3) abgeleiteten Chiffre

e n v o y e z	u n b a t a i	l l o n i n f	a n t e r i e
1 4 5 1 5 1 5	2 4 1 2 5 2 3	4 4 1 4 3 4 2	2 4 5 1 1 3 1
5 3 3 2 4 5 5	2 3 1 1 2 1 3	1 1 2 3 3 3 5	1 3 2 5 3 3 5
14 51 51 55 33 24 55	24 12 52 32 31 12 13	44 14 34 21 12 33 35	24 51 13 11 32 53 35
D S S Z I C Z	C O T H G O R	P D J A O I K	C S R B H V K

Delastelle war praktisch erfahren genug, um die *longueur de sériation* nicht zu groß zu wählen: Ein Chiffrierfehler wirkt sich sonst (s. 11.3) über die ganze Nachricht aus. Aber die Gefahr der unbefugten Entzifferung wächst.

[5] *Félix Marie Delastelle*, 1840–1902. Verfasser des *Traité Élémentaire de Cryptographie*, Gauthier-Villars, Paris 1902.

9.4.7 *Delastelle* diskutierte auch tomographische Verfahren auf der Basis einer tripartiten Substitution (vgl. 4.1.3). Andere tomographische Verfahren benutzen die ternäre Morse-Codierung, so ein POLLUX genanntes Verfahren und ein ‚revertiertes Kulissenverfahren' von *M. E. Ohaver*, das im nachfolgenden Beispiel die Chiffrierbreite 7 hat:

	s	e	n	d	s	u	p
	···	·	–·	–··	···	··–	·––·
Codelänge	3	1	2	3	3	3	4
revertiert	4	3	3	3	2	1	3
umgruppierte Zeichen	····	–·–	···	···	·–	·	––·
	H	K	S	S	A	E	G

9.5 Durchmischung durch arithmetische Operationen

Eine gründliche Durchmischung wird insbesondere durch arithmetische Operationen herbeigeführt. Eine bei Mathematikern beliebte Methode, die neuerdings wieder ausgegraben wurde (s. 10.3), ist die *monoalphabetische* Blockchiffrierung einer Nachricht als Zahl und anschließende Chiffrierung dieser Zahl durch arithmetische Operationen *modulo* einer geeigneten Zahl q, eventuell mit schließlicher Rückchiffrierung (‚symbolische Addition', ‚symbolische Multiplikation').

Die stellenweise Addition liegt schon den linearen Transformationen zugrunde, man kann aber auch die ganze Nachricht (nach Überführung in eine Zahl) zur Chiffrierung Operationen wie Addition eines Additivs, Multiplikation mit einem regulären Faktor h (vgl. 5.7) oder r-fache Potenzierung — alles *modulo* q — unterwerfen. Dies sind Operationen, deren Inverse (zur berufenen Dechiffrierung) mit etwa dem gleichen Aufwand auskommen und in steigendem Maße Durchmischung bedeuten: die Multiplikation als iterierte Addition, die Potenzierung als iterierte Multiplikation.

Bei gegebenem q kann damit eine Nachricht chiffriert werden, deren Zahläquivalent x der Bedingung $0 \le x < q$ genügt. Die zugehörige Chiffrierung als Zahl kann beispielsweise durch landläufige Codebücher erfolgen, wobei bereits eine Komprimierung eintritt, die bei stereotypen Texten beträchtlich sein kann: Bei Handelscodes kann man mindestens mit durchschnittlich 8.5 Buchstaben Klartext pro Ziffern-Fünfergruppe rechnen. Die Methode eignet sich insbesondere zur Blockchiffrierung.

Die Codierung als Zahl kann auch in einem Zahlsystem zur Basis B, $B > |V|$ erfolgen — für $V = \mathbb{Z}_{26}$ etwa zur Basis 100, also wesentlich dezimal ($\mathbb{Z}_{10}^2$) mit Ziffernpaaren, oder zur Basis 32, also wesentlich binär wie im Fernschreibcode ($\mathbb{Z}_2^5$) mit Fünf-Bit-Gruppen.

Heute werden überwiegend Bytes ($B = 256$), 16-Bit-Gruppen ($B = 2^{16}$), 32-Bit-Gruppen ($B = 2^{32}$) und 64-Bit-Gruppen ($B = 2^{64}$) herangezogen.

9.5.1 Symbolische Multiplikation mit einem Faktor h *modulo* q:

$$M_h(x) = x \cdot h \mod q .$$

Ist $q{=}p$ prim, so bildet die Multiplikation *modulo* p eine Gruppe, es gibt zu jedem $h \not\equiv 0 \mod p$ ein Inverses h' so daß $h \cdot h' \mod p = 1$, und es ist

$$M_{h'}(M_h(x)) = x \qquad \text{(Multiplikation in } \mathbb{F}(p)) .$$

Ist q nicht prim, so hat h nur dann ein Inverses (ist regulär), wenn es zu q teilerfremd ist (vgl. 5.6).

Aus technischen Gründen verwendet man häufig q von der Form $q = 2^k$ oder $q = 2^k - 1$, wenn die Berechnung im Dualsystem erfolgt; im Dezimalsystem entsprechend $q = 10^k$ oder $q = 10^k - 1$. Im Falle $q = 2^k$ bzw. $q = 10^k$ fällt bei Rechnung mit der Wortlänge k das Ergebnis im hinteren Teil des (dualen bzw. dezimalen) Akkumulators an, vgl. 5.7. Im Falle $q = 2^k$ haben nur die ungeraden Zahlen Inverse, im Falle $q = 2^k - 1$ sind nicht-prime q zu vermeiden, man ist auf Mersenne-Primzahlen beschränkt.

Bei größeren Werten von q scheint die Bestimmung der Reziproken h' zu gegebenem h nicht mehr trivial zu sein. Der Divisionsalgorithmus durch sukzessive Subtraktion funktioniert jedoch auch für Zykelzahlen (5. Kapitel) und terminiert genau dann, wenn es einen Quotienten gibt. Ein Analogon zu dem schnellen Divisionsalgorithmus, den wir gewohnheitsmäßig für $\mathbb{Z}$ in einem Stellenwertsystem durchführen, existiert ebenfalls, vgl. 5.7. Er kann auch in der Form durchgeführt werden, die folgendes Beispiel zeigt:

$17 \cdot h' \equiv 1 \mod 1\,000$

$$\begin{array}{rl} -1 & \\ 16 & \\ 33 & \\ 5\mathbf{0} & \left.\right\} 3 \\ 220 & \\ 390 & \\ 560 & \\ 730 & \\ 9\mathbf{0}0 & \left.\right\} 5 \\ 2600 & \\ 4300 & \\ 6\mathbf{0}00 & \left.\right\} 3 \end{array} \qquad 17 \cdot 353 = 6001 \equiv 1 \mod 1\,000 .$$

Es ist ein leichtes, einen Mikroprozessor entsprechend effizient zu programmieren. Ist aber das Reziproke h' bestimmt, so erfordert die Dechiffrierung den gleichen Aufwand wie die Chiffrierung.

Ist q etwa Produkt zweier (verschiedener) Primzahlen $q = p_1 \cdot p_2$, und ist $h \cdot h'_1 \equiv 1 \mod p_1$ und $h \cdot h'_2 \equiv 1 \mod p_2$, so ist $h \cdot h' \equiv 1 \mod q$, wo $h' \equiv h'_1 \mod p_1$ und $h' \equiv h'_2 \mod p_2$.

Die Restklassenarithmetik reduziert hier den Arbeitsaufwand zur Bestimmung von h' beträchtlich.

9.5.2 Symbolische Potenzierung mit einem Exponenten k *modulo* q:

$$P_k(x) = x^k \mod q\,.$$

Satz. Sei $q = p$ eine Primzahl. Ist k' derart, daß $k \cdot k' \equiv 1 \mod p-1$, so ist zu $P_k(x) = x^k \mod p$ invers $P_{k'}(x) = x^{k'} \mod p$, und es ist

$$P_{k'}(P_k(x)) = x \qquad (\text{ Potenzierung in } \mathbb{F}(p))\,.$$

Beweis: Zunächst ist

$$\begin{aligned} P_{k'}(P_k(x)) &= x^{k\cdot k'} \bmod p = x^{k\cdot(k' \bmod (p-1) + \alpha\cdot(p-1))} \bmod p \\ &= x^{k\cdot k' \bmod (p-1)} \cdot x^{k\alpha\cdot(p-1)} \bmod p \qquad \text{für geeignetes } \alpha \\ &= x^1 \cdot (x^{p-1} \bmod p)^{k\alpha} \end{aligned}$$

Nach dem kleinen Fermatschen Satz ist aber

$x^{p-1} \bmod p = 1$, somit

$P_{k'}(P_k(x)) = x$. ⋈

Beispiele: Gegenseitig reziproke nichttriviale Paare $(k\,,k')$ können in 5.5, Tabelle 1 gefunden werden, z.B.

für $p = 11$: (3,7) und (9,9) $(N{=}10)$;
für $p = 23$: (3,15), (5,9), (7,19), (13,17) und (21,21) $(N{=}22)$;
für $p = 31$: (7,13), (17,23), (11,11), (19,19) und (29,29) $(N{=}30)$.

Fall $p = 11$:

$x^3 \bmod 11$ hat die Zyklendarstellung (0) (1) (2 8 6 7) (3 5 4 9) (10) ,
$x^9 \bmod 11$ hat die Zyklendarstellung (0) (1) (2 6) (8 7) (3 4) (5 9) (10) .

$x \bmod 11$, $x^3 \bmod 11$, $x^9 \bmod 11$, and $x^7 \bmod 11$ bilden die zyklische Gruppe $\mathcal{C}_4$ der Ordnung 4.

Fall $p = 31$:

$x^7 \bmod 31$ hat die Zyklendarstellung A der Ordnung 4
(0) (1) (5) (25) (9 10 20 18) (17 12 24 3) (2 4 16 8)
(6) (26) (14 19 7 28) (22 21 11 13) (15 23 29 27) (30)
$x^{11} \bmod 31$ hat die Zyklendarstellung B der Ordnung 2
(0) (1) (5) (25) (9 14) (10 19) (17 22) (12 21) (2) (16) (4) (8)
(6) (26) (20 7) (18 28) (24 11) (3 13) (15) (29) (23) (27) (30)
$x^{17} \bmod 31$ hat die Zyklendarstellung AB der Ordnung 4
(0) (1) (5) (25) (14 10 7 18) (22 12 11 3) (2 4 16 8)
(6) (26) (9 19 20 28) (17 21 24 13) (15 23 29 27) (30)
$x^{19} \bmod 31$ hat die Zyklendarstellung A^2 der Ordnung 2
(0) (1) (5) (25) (9 20) (10 18) (17 24) (12 3) (2 16) (4 8)
(6) (26) (14 7) (19 28) (22 11) (21 13) (15 29) (23 27) (30)

x^{29} mod 31 hat die Zyklendarstellung A^2B der Ordnung 2
(0) (1) (5) (25) (9 7) (10 28) (17 11) (12 13) (2 16) (4 8)
(6) (26) (14 20) (19 18) (22 24) (21 3) (15 29) (23 27) (30)
x^7 mod 31 and x^{29} mod 31 erzeugen die Gruppe $\mathcal{C}_4 \times \mathcal{C}_2$ der Ordnung 8.

Fall $p = 23$:
x^7 mod 23 hat die Zyklendarstellung
(0) (1) (2 13 9 4 8 12 16 18 6 3) (5 17 20 21 10 14 19 15 11 7) (22) und erzeugt die zyklische Gruppe $\mathcal{C}_{10}$ der Ordnung 10.

Ist q ein Produkt zweier (verschiedener) Primzahlen, $q = p_1 \cdot p_2$, so gilt ein leicht abgeänderter Satz (s. 10.3.1).

Für eine ungerade Primzahl p bildet die Menge $\{P_h : h$ regulär bzgl. $p-1\}$ eine Abelsche (kommutative) Gruppe $\mathcal{M}_{p-1}$, abhängig von p. Polyalphabetische Chiffrierung mit dieser Gruppe als Schlüsselgruppe ist möglich. Die Gruppe ist von der Ordnung $\frac{p-1}{2} - 1$, wenn $\frac{p-1}{2}$ prim ist.

Eine ungerade Primzahl p derart daß $p' = \frac{p-1}{2}$ ebenfalls eine Primzahl ist, wird eine **sichere** (oder **starke**) Primzahl (*Bob* und *G. R. Blakely* 1978) genannt (p' wird dann auch als *Sophie-Germain*-Primzahl bezeichnet).

Sichere Primzahlen sind 5, 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467, 479, 503, 563, 587, 719, 839, 863, 887, 983, 1019, 1187, 1283, 1307, 1319, 1367, 1439, 1487, ... ; es gibt auch große wie $45 \cdot 2^{37} - 1$ und $10^{100} - 166517$. Abgesehen von 5 und 7 sind alle sicheren Primzahlen von der Form $12a - 1$.

$P_h(x)$ hat den trivialen Fixpunkt $x = 0$ und die zwei normalen Fixpunkte $x = 1$, $x = p-1$, neben möglicherweise anderen. Die Potenzen $P_h(x)$, $P_{h'}(x)$ können gebildet werden als Produkte wiederholter Quadrate; eine Binärdarstellung von k und k' zeigt, wie dies zu geschehen hat.

Für $p{=}11$, da $3 = \mathbf{L\,L}$ und $7 = \mathbf{L\,L\,L}$; $9 = \mathbf{L\,O\,O\,L}$:

$$P_3(x) = x \cdot x^2 , \qquad P_7(x) = x \cdot x^2 \cdot (x^2)^2 , \qquad P_9(x) = x \cdot ((x^2)^2)^2 ,$$

wo $\cdot\,\cdot\,\cdot$ Multiplikation und $.^2$ Quadrierung, beide *modulo* 11, anzeigt.

In der Tat braucht für n-Bit-Primzahlen p mit $2^n < p < 2^{n+1}$ die Potenzierung *modulo* p ungefähr den gleichen Aufwand wie n Multiplikationen. Mit der gegenwärtigen Tendenz, Chiffrierschritte in Mikroprozessorchips zu verlagern, werden arithmetische Methoden zukünftig mehr und mehr Bedeutung erlangen. Speziell für Primzahlen der Form $p = 2^{2^k} + 1$ (Fermatsche Primzahlen) kommt man zum Problem reziproker Paare *modulo* 2^{2^k}, wofür es spezielle Lösungen gibt.

9.5.3 Wegen der Vertauschbarkeit von h und h' in 9.5.1 und 9.5.2 kann im wechselseitigen Verkehr zweier Partner A und B der eine h, der andere h' jeweils zum Chiffrieren *und* zum Dechiffrieren verwenden. Mittels einer Menge von Paaren $(h_i\,, h_i{}')$ ist auch polyalphabetische Chiffrierung möglich (vgl. 2.6.2).

9.5.4 Vorläufer für diese arithmetischen Methoden ist *Pliny Earle Chase*, der 1859 im neugegründeten Mathematical Monthly folgendes Verfahren beschrieb: Nach einer bipartiten Substitution $V \to W^2$ mit $W = Z_{10}$ wird, wie bei *Mirabeau*, (vgl. 9.4.4) aus den jeweils ersten und den jeweils zweiten Ziffern eine Zahl x und eine Zahl y gebildet; nach einer einfachen arithmetischen Operation, wie etwa y mit Neun zu multiplizieren, wird in V zurückübersetzt. Dieses einfache System bot mehr Sicherheit als vieles, was zu dieser Zeit in Gebrauch war; es fand aber keine praktische Verwendung.

9.6 DES und IDEA®

DES (Data Encryption Standard) wurde 1977 vom National Bureau of Standards (NBS) in den U.S.A. zur Verwendung für *"unclassified computer data"* genormt.[6] Das Verfahren liefert eine Blockchiffrierung für Byte-Oktogramme. Eine Folge von festen Transpositionen und von schlüsselabhängigen, multipartiten, nichtlinearen Substitutionen sorgt für eine sehr gründliche Durchmischung. DES ist ein tomographisches Verfahren, was man besonders gut am ursprünglichen Vorschlag LUCIFER von *Horst Feistel* (Abb. 76) sieht. Der Schlüssel ist 8 Byte lang, wovon noch die 8 Paritätsbits ‚abzuziehen' sind, die auf Drängen von N.S.A. eingeführt wurden. Die effektive Schlüssellänge ist also 56 Bit. Die Patenschaft von *Shannon* (9.4) ist unverkennbar.

9.6.1 Der DES-Algorithmus

Wir skizzieren an dieser Stelle nur den Ablauf des Verfahrens. Für Einzelheiten sei auf die erwähnte Publikation[8] verwiesen.

9.6.1.1 Chiffrieren

Der prinzipielle Ablauf eines DES-Chiffrierschrittes ist in Abb. 77 dargestellt: Der 8-Byte-Klartextblock wird zunächst einer (schlüsselunabhängigen) Eingangstransposition T unterworfen und anschließend in zwei 4-Byte-Blöcke L_0 und R_0 aufgeteilt. Nun folgen 16 Runden $(i = 1, 2, 3, \ldots, 16)$ mit

$$L_i = R_{i-1} \quad \text{und} \quad R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \quad ,$$

Das Zeichen $\oplus$ steht für die Addition *modulo* 2. K_i ist ein 48-Bit-Schlüssel, der über eine Auswahlfunktion aus dem vorgegebenen Schlüssel erzeugt wird. Den Abschluß bildet die zu T inverse Ausgangstransposition T^{-1}.

Die Funktion f bestimmt den zentralen Teil des Verfahrens (Abb. 78). Der 32-Bit-Block R_{i-1} wird durch Duplizierung bestimmter Bitstellen zu einem 48-Bit-Block $E(R_{i-1})$ expandiert und *modulo* 2 zu K_i addiert. Das

---

[6] Data Encryption Standard (DES), National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 46, National Technical Information Service, Springfield, VA, Apr. 1977. Federal Register, March 17, 1975 und August 1, 1975. Für die Darstellung von Hintergrundinformation (aus der Sicht von NBS) sei verwiesen auf: *Smid, M. E.*; *Branstad, D. K.*: The Data Encryption Standard: Past and Future, Proceedings of the IEEE, Vol. 76, No. 5, May 1988.

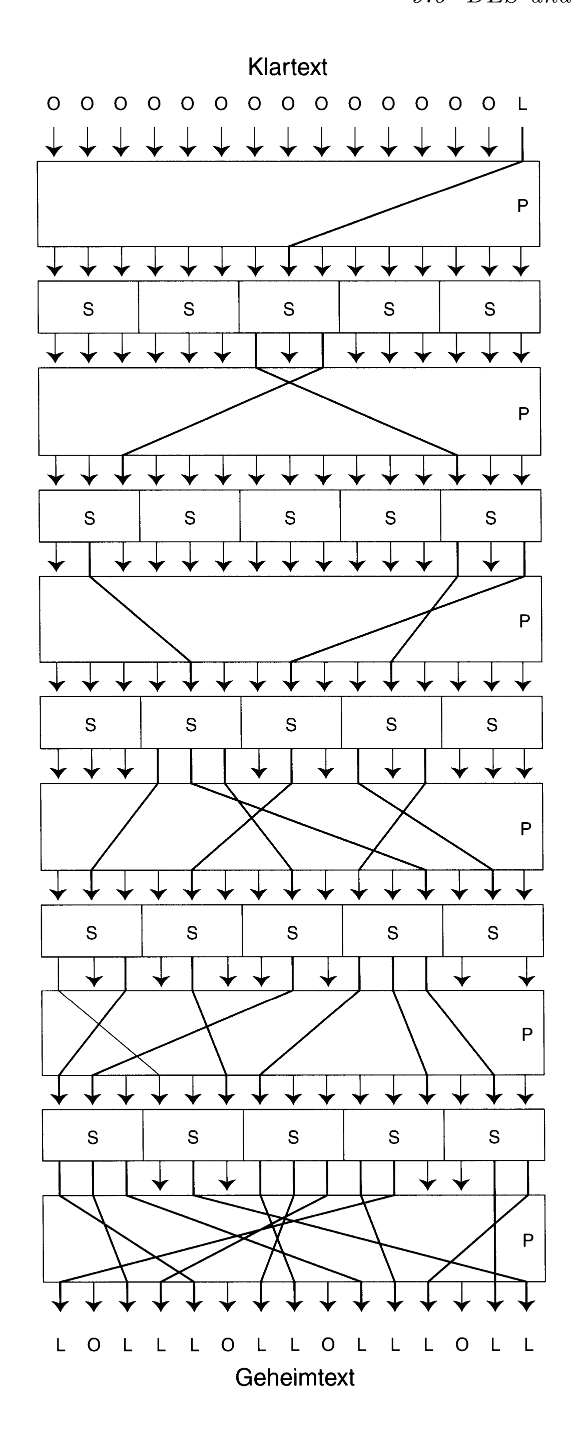


Abb. 76. LUCIFER-Chiffrierung (*nach Horst Feistel* 1973). Ein Klartext, der nur ein einziges **L** (und 14 **O**) enthält, wird durch die nichtlinearen Substitutionsmoduln lawinenartig in einen Geheimtext aus elf **L** (und vier **O**) überführt.

Abb. 77.
DES-Chiffrierschritt

Ergebnis wird in acht 6-Bit-Gruppen aufgeteilt, die als Eingabe für jeweils einen der 8 Substitutionsmoduln S_1 , S_2 bis S_8 (‘*S-boxes*’) dienen. Diese Moduln realisieren jeweils 4 verschiedene nichtlineare Substitutionen. In der folgenden Tabelle sind diese Substitutionen beispielsweise für S_1 dargestellt:

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
S_1:	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Bit 1 und 6 der jeweiligen Eingabe bestimmen — als Dualzahl interpretiert — die Zeile (und damit die Substitution), die Bits 2 bis 5 die Spalte. Die Eingabe 110010 (Zeile 2, Spalte 9 in der Tabelle) führt beim Modul S_1 also zur Ausgabe der Bitfolge 1100. Die acht 4-Bit-Ausgabeblöcke der Substitutionsmoduln S_1 , S_2 bis S_8 werden konkateniert und einer abschließenden Transposition P ('*P-box*') unterworfen.

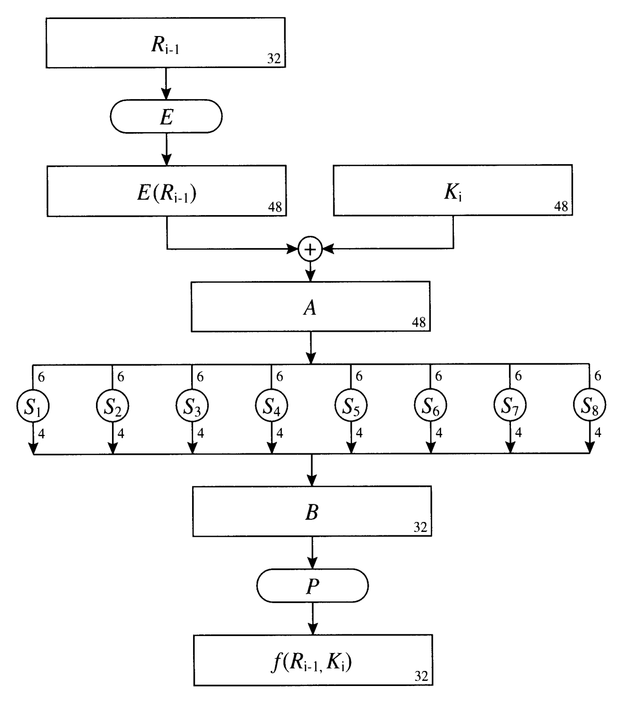


Abb. 78. Die Funktion f

Es bleibt noch die Frage nach der Herleitung der Teilschlüssel. Zunächst werden die Paritätsbits des vom Benutzer vorgegebenen Schlüssels entfernt, die verbleibenden 56 Bits werden nach einer festen Vorschrift permutiert und in zwei 28-Bit-Blöcke aufgeteilt. Diese Blöcke werden bei jeder Runde zyklisch um eine oder zwei Positionen — abhängig vom Rundenindex — nach links geschiftet. Aus beiden wird dann nach einem vorgegebenen Verfahren ein 48-Bit-Teilschlüssel (K_i) generiert.

9.6.1.2 Dechiffrieren

Für das Dechiffrieren wird der gleiche Algorithmus angewandt, wobei die Teilschlüssel (K_i) jetzt aber in umgekehrter Reihenfolge zum Einsatz kommen. Zum Chiffrieren und Dechiffrieren dient also der gleiche Schlüssel, der Algorithmus ist im weiteren Sinn **schlüsselsymmetrisch**. Die einzelnen Runden des Chiffrierens können nämlich durch die involutorischen Abbildungen

$$h_i : (R\ ,\ L) \longmapsto (R\ ,\ L \oplus f(R\ ,\ K_i)) \quad \text{(Verarbeiten)}$$
$$g\ : (R\ ,\ L) \longmapsto (L\ ,\ R) \quad \text{(Vertauschen)}$$

beschrieben werden. Bei g ist die Involution offensichtlich, bei h_i folgt sie aus der Beziehung

$$L \oplus f(R\ ,\ K_i) \oplus f(R\ ,\ K_i) = L\ .$$

Das Chiffrieren führt also insgesamt auf die Abbildung

$$DES \equiv T^{-1} \circ h_{16} \circ g \circ h_{15} \circ g \circ\ \ldots\ \circ h_2 \circ g \circ h_1 \circ T$$

(bei der letzten Runde wird nicht mehr vertauscht). Beim Dechiffrieren wird lediglich die Reihenfolge der Teilschlüssel umgekehrt:

$$DES^{-1} \equiv T^{-1} \circ h_1 \circ g \circ h_2 \circ g \circ\ \ldots\ \circ h_{15} \circ g \circ h_{16} \circ T$$

Die Komposition von DES und DES^{-1} ergibt wegen der Involution der einzelnen Abbildungen die identische Abbildung.

9.6.2 ‚Lawinen'-Effekt

Man kann zeigen, daß bereits nach wenigen Runden jedes Bit des ‚Zwischenergebnisses' von jedem Bit des Klartextblockes und jedem Bit des Schlüssels abhängt. Minimale Änderungen des Klartextblockes bzw. des Schlüssels bewirken deshalb, daß sich etwa 50 % der Bitpositionen des Chiffrats ändern (‚Lawineneffekt').

9.6.3 Betriebsmodi von DES

Sollen mehr als acht Byte chiffriert werden, so ist der Klartext in eine Folge von 8-Byte-Blöcken aufzuspalten. Der Klartext kann andererseits bei manchen Anwendungen in der Regel auch weniger als acht Byte umfassen, wenn zum Beispiel die Information sequentiell anfällt und ohne Zeitverlust übertragen werden muß. Für beide Fälle sind unterschiedliche Betriebsweisen denkbar, die sich in bezug auf Chiffriergeschwindigkeit und Fehlerfortpflanzung wesentlich unterscheiden können. Letztlich entscheidet die vorgesehene Anwendung über die Eignung der Alternativen.

Das *National Institute of Standards and Technology* (N.I.S.T.), früher *National Bureau of Standards* (N.B.S.) hat in den U.S.A. vier verschiedene Betriebsweisen genormt – je zwei für die oben genannten grundsätzlichen Anwendungsfälle.[7]

Beim ECB-Modus (*Electronic Code Book*) werden die einzelnen 8-Byte-Blöcke unabhängig voneinander chiffriert. Gleiche Klartextblöcke führen dabei zu gleichen Geheimtextblöcken. Dieser Modus mit seinem streng monoalphabetischen Einsatz von DES sollte nach Möglichkeit vermieden werden.

[7] DES Modes of Operation, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 81, National Technical Information Service, Springfield, VA, Dec. 1980.

Beim CBC-Modus (*Cipher Block Chaining*) werden die Blöcke miteinander verkettet. Ausgangspunkt ist ein (zwischen den Partnern zu vereinbarender) Initialisierungsblock c_0 (*session key*).

Die Chiffrierung der Klartextblöcke m_1 , m_2 , m_3 , ... führt zu folgenden Geheimtextblöcken c_1 , c_2 , c_3 , ... mit

$$c_1 = DES(m_1 \oplus c_0) \qquad c_2 = DES(m_2 \oplus c_1) \qquad c_3 = DES(m_3 \oplus c_2)$$

Die Dechiffrierung erfolgt über

$$m_1 = DES^{-1}(c_1) \oplus c_0 \quad m_2 = DES^{-1}(c_2) \oplus c_1 \quad m_3 = DES^{-1}(c_3) \oplus c_2$$

Die Chiffrierung ist jetzt zwar polyalphabetisch, aber mit einer sehr „regelmäßigen“, an einen *autokey* erinnernden Auswahl der Alphabete.

Neben diesen blockorientierten direkten Chiffrierungen ist noch normiert der CFB-Modus (*Cipher Feedback*), bei dem DES nicht direkt zur Chiffrierung, sondern nur zur Erzeugung von Pseudozufallszahlen verwendet wird, mit einer Wahlmöglichkeit zwischen 1-Bit-, 8-Bit-, 16-Bit-, 32-Bit- und 64-Bit-Resultaten, mit der Variante OFB-Modus (*Output Feedback*) für 64-Bit-Resultate, die einen vom Klartext- und vom Geheimtextstrom unabhängigen Rückkopplungsmechanismus besitzt. Sie wird für Authentisierung benützt.

9.6.4 Zur Sicherheit von DES

Seit den ersten Veröffentlichungen des vorgesehenen und später auch realisierten Standards hat es um den DES-Algorithmus Diskussionen und Kritik gegeben. So wurde z. B. verschiedentlich die Anzahl der internen Runden mit 16 als zu gering empfunden. Die Hauptangriffspunkte sind:

- Die Design-Kriterien der S-Boxen wurden zunächst gar nicht, später nur sehr vage bekanntgegeben; schließlich wurden sie nach 1990 von *Donald Coppersmith* publiziert. Diese für die Sicherheit zentralen Barrieren könnten ‚Falltüren‘ enthalten, die den Entwicklern von DES die (unbefugte) Invertierung zumindest wesentlich erleichtern.
- Die Schlüssellänge ist mit acht Byte relativ klein. Nach ‚Abzug‘ der 8 Paritätsbits verbleiben gerade noch 56 frei verfügbare Binärstellen. Es sind also nur 2^{56} verschiedene Schlüssel wählbar (beim ursprünglichen Entwurf LUCIFER – und dieser Vergleich ist sicher naheliegend – ist die Anzahl der Schlüssel mit 2^{128} wesentlich größer).
- Der Schlüssel wird jeweils für eine Verbindung gewählt und bleibt dann vergleichsweise sehr lange fest – dieser praktisch monoalphabetische Gebrauch von DES fordert den klassischen Angriff der Superimposition (s. 19.1) geradezu heraus.

Andrerseits ist DES ein ziemlich schneller Chiffrieralgorithmus. Größere Schlüssellänge, mehr Runden und andere Sicherheitsmaßnahmen würden den Chip langsamer machen. Die weltweite Akzeptanz von DES als ein *de facto* Standard rechtfertigen einigermaßen den Entwurf.

Teilweise wurde diese Diskussion geführt vor einem Hintergrund tiefen Mißtrauens: Das N. I. S. T. wurde verdächtigt und sogar insgeheim beschuldigt, als verlängerter Arm der *National Security Agency* zu wirken, von der man annahm, daß sie ein Interesse habe, Chiffrierungen brechen zu können. Offizielle Verlautbarungen waren nicht geeignet, den Verdacht auszuräumen.

Es sind zwar immer noch keine Falltüren (öffentlich) bekannt. Es gibt aber andererseits auch keinen Nachweis für deren Nichtexistenz. Es wurden auch einige überraschende Eigenschaften des DES-Algorithmus gefunden, wie etwa eine Symmetrie unter Komplementierung: Wenn sowohl Klartext wie Schlüssel komplementiert werden, ist der resultierende Geheimtext ebenfalls komplementiert. Es könnte andere, bisher unentdeckte Symmetrien geben. Ein Rest von Sorge bleibt deshalb nach wie vor erhalten.

Jedenfalls ist zu hoffen, daß mit massiver Unterstützung durch übergroße Rechner DES gebrochen werden kann, wenn die Weltsicherheit es erfordert. Für private Initiativen sollte DES unangreifbar sein und ist es höchstwahrscheinlich auch, wenn es diszipliniert gebraucht wird.

Wer sich jedoch Sorgen um die Sicherheit von DES macht, sollte jedenfalls nicht den ECB-Modus verwenden, von dem seit langem abgeraten wird, der aber von unzuverlässigen Anbietern nach wie vor in den Handel gebracht wird. Er kann weiterhin versuchen, der geringen Schlüssellänge mit mehrfacher DES-Chiffrierung mittels voneinander unabhängiger Schlüssel zu begegnen. Es besteht jedoch die Gefahr einer *complication illusoire*.

Eine obere Grenze für den Aufwand, der zum Brechen einer Chiffrierung notwendig ist, gibt der *“brute force”* Angriff. Man sollte daher im Auge behalten, daß DES für unbegrenzte Versuche durch jedermann für beliebig lange Zeit verfügbar ist. *Eli Biham* und *Adi Shamir* haben 1993 eine generell gegen Durchmischungsverfahren gerichtete Methode angegeben, die bestimmte kleine Abänderungen des Klartextes benützt (‘*Differential Cryptanalysis*’). Es stellt sich heraus, daß dabei für DES der verbleibende *“brute force”* Angriff durchschnittlich „nur“ 2^{47} Versuche (gegenüber 2^{56} bei voller Exhaustion) erforderlich macht. Das ist zwar nur von theoretischem Interesse, aber doch verlockend. *Donald Coppersmith* hat dann aufgedeckt, daß bereits 1974 beim Entwurf von DES bestmögliche Vorkehrungen gegen einen derartigen Angriff getroffen wurden.

Für DES sind seit etwa 1980 spezielle Chips auf dem Markt. Damit lassen sich nach dem Stand der ersten Hälfte der 90er Jahre 10–20 Mbits/sec chiffrieren und dechiffrieren. Abb. 79 zeigt einen Chip aus der Anfangszeit (1979).

Das DES-Verfahren hat sich (trotz Exportbeschränkungen) weltweit ohne Zwang durchgesetzt, indem es zum Marktführer wurde. Dies muß die *National Security Agency* (N.S.A.) der U.S.A. mit Befriedigung erfüllen. Wie weit eventuellen Nachfolgern von DES solches gleichermaßen gelingen wird, bleibt abzuwarten.

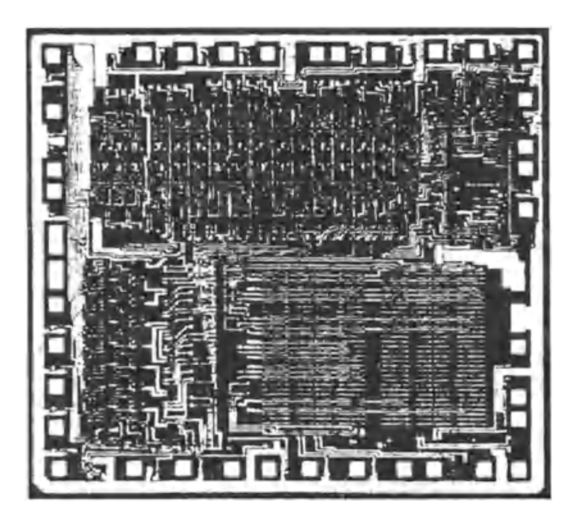


Abb. 79. DES-Chip (1979)

9.6.5 Nachfolger für DES

Frei exportierbar, weil unsicher, sind die 1993 auf den Markt gebrachten 40-Bit-Algorithmen RC2 und RC4 der Firma RSA Data Security, Inc. "*If you get permission from the U.S.* [for a license to export an encryption algorithm] *that probably means it's too easy to decrypt.*" (Ralph Spencer Poore). Die zwischenzeitlich weitverbreitete Meinung (*Otto Horak, 1996*: "*DES is nearing the end of its credibility*"), daß das 56-Bit-DES, das 1977 nur für eine Dekade gedacht war, bald abgelöst werden muß – schließlich fand in den 20 Jahren von 1977 bis 1997 eine Steigerung der maximalen Rechenleistung etwa um den Faktor 2^{10} statt – wurde 1998 unterstützt durch gelungene *brute force*-Einbrüche exhaustiver Art. Daraufhin zog im Januar 1999 das N.I.S.T. (National Institute of Standards and Technology) seine Unterstützung von DES zurück und empfahl im Februar 1999 als Übergangslösung bis zu einer in einigen Jahren zu erwartenden Einführung eines neuen *Advanced Encryption Standard* (AES) ein ‚TripleDES' (FIPS 46-3) mit 168 Bit, das allerdings die dreifache Zeit zur Chiffrierung oder Dechiffrierung braucht.

Eine äußerliche Verbesserung gegenüber DES bringt der SKIPJACK-Algorithmus, der, ebenfalls schlüsselsymmetrisch, mit einem Schlüssel von 80 Bits in 32 Runden arbeitet. Würde man 1993 mit einem Spezialcomputer[8] für $ 100 000 zur Exhaustion der Schlüsselmenge von DES 3.5 h gebraucht haben, so wäre diese Leistung mit gleichem Aufwand erst 2029 für SKIPJACK erreichbar; 1993 würde man mit diesen Mitteln noch $26.2 \cdot 2^{20}$ Jahre, 2005 jedoch nur noch $6.55 \cdot 2^{10}$ Jahre und 2017 1.64 Jahre brauchen – und dies für den rein exhaustiven (*brute force*) Angriff; jeder standesbewußte Kryptanalytiker würde sich etwas einfallen lassen, um es schneller zu machen.

[8] nach *M. J. Wiener*, Efficient DES Key Search. CRYPTO '93, Santa Barbara, CA, Aug. 22-26, 1993.

SKIPJACK war jedoch aufgrund U.S.-amerikanischer Gesetze bis Juni 1998 nur als eingriffsresistenter, von Mykotronx, Torrence, Calif., USA programmierter Chip MYK-78 (im CLIPPER-System), mit einem Durchsatz bis 20 MBits/sec und einem Preis von einigen zehn Dollar, und nicht als Software erhältlich. Damit war insbesondere seine Verwendbarkeit in Rechnernetzen sehr eingeschränkt, von handelspolitischen und anderen (die Grundrechte betreffenden) Erwägungen ganz abgesehen. Die Rolle als *de facto* Standard, die DES hatte, dürfte SKIPJACK auch nach seiner Offenlegung nicht erreichen.

Das gemeinhin liberalere Europa bindet sich nicht an das Vorgehen der U.S.-Regierung. Unter den verschiedenen freien Ansätzen zur Ablösung von DES ist vielleicht am aussichtsreichsten IDEA® (*International Data Encryption Algorithm*), von *J. L. Massey* und anderen seit 1990 entwickelt, patentiert und für die Schweizer Firma ASCOM TECH AG, Solothurn unter Markenschutz stehend, der seit 1993 in CMOS-Technik als VLSI-Chip und als Software unbehindert erhältlich ist. Handelsbeschränkungen sind nicht bekannt. IDEA® mit einem Schlüsselraum von 128 Bits ist für das nächste Jahrzehnt einem *"brute force"* Angriff gewachsen – anderen Einbruchsmöglichkeiten ist der Algorithmus selbstverständlich ebenso ausgesetzt wie SKIPJACK und DES. – Alle diese Chiffrieralgorithmen arbeiten mit 8-Byte-Klartextblöcken.

Gelegentlich werden allerdings nicht alle vorhandenen Bits kryptologisch ausgenutzt. So stellte sich Anfang 1998 heraus, daß in einem weltweit zur Absicherung des Zugangs zu GSM-Mobilfunk-Telefonen (D1, D2, E-plus) verwendeten 64-Bit-Schlüssel die letzten zehn Bits ständig mit **O** besetzt waren. Ein *brute force*-Angriff wird damit um den Faktor Tausend kürzer und reicht in den Stunden-bis-Tage-Bereich des Zeitaufwands.

9.6.6 Kryptosysteme und Kryptochips

Viel Aufsehen erregte ein Kryptosystem, das sich ab Mitte 1991 weltweit verbreitete, genannt PGP® ('*Pretty Good Privacy*', scherzhaft auch '*Pretty Good Piracy*'); ein Paket, das neben der Chiffrierung und Dechiffrierung (Algorithmen von IDEA®, neuerdings auch TripleDES und andere) auch Maßnahmen zur gesicherten Schlüsselvereinbarung und Signatur (Algorithmen von RSA, siehe 10.3, sowie Algorithmen von MD5 und SHA[9]) enthält. PGP ist in erstaunlich kurzer Zeit ein *de-facto*-Standard für *e-mail* über das *Internet* geworden. PGP entwich seinem Schöpfer, *Philip R. Zimmermann* und schlüpfte damit durch die Maschen der Gesetze der U.S.A., sehr zum Mißvergnügen der N.S.A., begleitet von der Schadenfreude einer weltweiten Cypherpunks-Bewegung. Ob *Zimmermann* nach den U.S.-Gesetzen bestraft werden kann oder soll, war lange nicht klar. Im Januar 1996 stellte jedoch das F.B.I. seine Ermittlungen gegen ihn ein. Inzwischen wurde PGP Software auch in den U.S.A. für $ 100 verkauft und ist derzeit für persönliche nichtkommerzielle Verwendung kostenfrei erhältlich.

---

[9] MD5: "Message Digest 5", ein Einweg-*hash*-Algorithmus zur Bildung von 128-Bit-Prüfgruppen. SHA: "Secure Hash Algorithm" zur Bildung von 160-Bit-Prüfgruppen, siehe 10.5.

Ohnehin können nationale Gesetze in einer Welt offener Grenzen nicht mehr viel Beachtung finden. Ein Beispiel gab im März 1998 Netscape mit der Freigabe ihres *WWW Software Communicator* "mozilla" im Quelltext. Um dem damaligen Exportverbot nach dem Kriegswaffengesetz der U.S.A. zu entsprechen, wurde der *secure sockets layer* (SSL), der sicheren Datenaustausch ermöglichen soll, ausgenommen. Binnen weniger Tage gab eine australische Quelle mit "cryptozilla" eine Version des Netscape Communicator heraus, die mit 128 Bit-Algorithmen zur Chiffrierung ausgestattet ist. Dies zeigt, warum die U.S. Regierung ein törichtes, den freien Welthandel schädigendes Gesetz nicht länger durchsetzen konnte.

Eine kritische Schwachstelle ist weiterhin die Schlüsselvereinbarung. Diese Lektion haben schon die Polen die Deutschen gelehrt. Würde jemand die Schlüsselvereinbarung brechen, wäre der ganze Chiffrieralgorithmus wertlos.

Mittlerweile werden Mikroprozessor-Chips immer leistungsfähiger. So arbeitete schon ein 1996 von Digital Equipment Corporation auf den Markt gebrachter 64-Bit-Prozessor-Chip Alpha-AXP (211 64) mit einer Pulsfrequenz von 300 MHz, beinhaltete 9.3 Millionen Transistoren und verarbeitete $1.2 \cdot 10^9$ Befehle pro Sekunde. Er wurde ursprünglich in 0.5μ-Technologie hergestellt, d.h. die elektrischen Verbindungen hatten eine Breite von 0.0005 mm. Bis 1999 wurde die Taktfrequenz erhöht; für den Nachfolger Alpha 212 64 auf rund 600 MHz unter Verwendung einer 0.35μ-Technologie. DEC hat für das Jahr 2000 Taktfrequenzen von über 1 GHz angekündigt und strebt eine 0.25μ- und eine 0.18μ-Technologie an.

Mikroprozessoren werden heute weithin verwendet, in Arbeits-, Tisch- und tragbaren Rechnern, und sind häufig in Nachrichtennetze eingebunden; umso mehr entsteht die Notwendigkeit, die übertragenen oder dem möglichen Zugriff sonstwie ausgesetzten Daten kryptologisch zu sichern. Crypto AG, Zug (Schweiz) hat 1996 ein *crypto board* für einzeln aufgestellte oder in ein Netz integrierte *desktop PCs* und *notebooks* auf den Markt gebracht, das neben Benutzer-Identifikation und Zugangskontrolle die Chiffrierung von Daten auf *hard disks* und *floppy disks*, von *directories* und von *files* mit einem Durchsatz von mindestens 38 Mbits/sec bereitstellt. Dieses *crypto board* hat seinen eigenen, eingriffsresistenten (*tamper-proof*) Schlüsselträger samt Kennwort-Speicher und arbeitet mit individuell erzeugten Pseudo-Zufalls-Schlüsseln in einem symmetrischen Blockchiffrierungs-Algorithmus. Die Schlüsselverwaltung benutzt eine mehrstufige Schlüsselhierarchie. *Master keys*, *data encryption keys*, *file keys* und *disk keys* haben eine Schlüsselmannigfaltigkeit von $2^{124} \approx 2.12 \cdot 10^{37}$. Mit den Abmessungen 85 mm mal 54 mm und nur 3.3 mm dick, ist das *crypto board* (Farbtafel P) extrem handlich. Nichtsdestoweniger, wenn es ordentlich gebraucht wird, kann man erwarten, daß es den Anstrengungen eines Supercomputers für eine geraume Zeit standhält.

‚Harte' Kryptographie lohnt sich, sie gewinnt deshalb mehr und mehr an Boden.

10 Öffentliche Chiffrierschlüssel

Die bisher diskutierten polyalphabetischen Chiffrierverfahren benötigten Schlüssel für die Chiffrierung und Schlüssel für die Dechiffrierung. Chiffrierschritt-Systeme mit involutorischen Chiffrierschritten benützen natürlicherweise den selben Schlüssel für beides. Andernfalls gibt es zwei Möglichkeiten:

(1) Es gibt nur einen Schlüssel, aber ein Schlüsselzeichen kann für die Chiffrierung eine andere Bedeutung haben als für die Dechiffrierung — kurz, *ein Schlüssel, zwei Regeln.* Dies ist für DES (9.6.1) der Fall.

Wenn man Chiffriermaschinen benützt, erfordert das ein Umschalten des Mechanismus zwischen dem Chiffrier-Modus und dem Dechiffrier-Modus.

(2) Es gibt sowohl einen Schlüssel für die Chiffrierung als einen Schlüssel für die für die Dechiffrierung — kurz, *zwei Schlüssel, eine Regel.*

Wenn man Chiffriermaschinen benützt, ist kein Umschalten des Mechanismus erforderlich, aber die Verfügbarkeit zweier Schlüssel. Wenn man von Hand arbeitet, hat man den Vorteil, nur eine Vorschrift beherrschen zu müssen. Wenn man jedoch nur den Chiffrierschlüssel geliefert bekommt, erfordert die Gewinnung des Dechiffrierschlüssels extra Mühe — außer es handelt sich um eine echt involutorische Chiffrierung.

Man kann das illustrieren am Beispiel des klassischen VIGENÈRE-Verfahrens mit der Chiffrierung E,

$$E = \{\chi_{k_j}\} : \quad \chi_{k_j}(x) \; = x + k_j \bmod N^n \, .$$

Fall (1) benutzt für die Dechiffrierung D

$$D = \{\chi_{k_j}^{-1}\} : \; \chi_{k_j}^{-1}(x) = x - k_j \bmod N^n \; ,$$

während Fall (2) dafür benutzt

$$D = \{\chi_{k_j}^{-1}\} : \; \chi_{-k_j}(x) = x + (-k_j) \bmod N^n \; .$$

Der Zusammenhang ist hier einfach genug,

$$\chi_{k_j}^{-1} = \; \chi_{(k_j)^{-1}} \quad \text{wobei} \quad (k_j)^{-1} = \; -k_j \, .$$

Entsprechend macht auch die Gewinnung des Dechiffrierschlüssels nur geringe Mühe, und da dieser geheimzuhalten ist, ist auch der Chiffrierschlüssel geheimzuhalten.

Wenn es aber ebensoviel Mühe machen würde, den Dechiffrierschlüssel $(k_j)^{-1}$ aus dem Chiffrierschlüssel k_j zu gewinnen, wie den Geheimtext auf irgend eine andere Weise zu brechen, könnte der Chiffrierschlüssel k_j ruhigen Gewissens veröffentlicht werden. In diesem Fall hätten wir ein **offenes Chiffrierverfahren**. Überraschenderweise existieren solche Chiffrierverfahren.

Die Frage stellt sich: Bietet ein solches Chiffrierverfahren mit einem öffentlichen Chiffrierschlüssel Vorteile? Und wenn so, warum taucht ein so einfacher Gedanke so spät – Mitte der siebziger Jahre – in der Geschichte der Kryptologie auf? Eine vorweggenommene Antwort lautet, daß offene kommerzielle Nachrichtennetze Eigenschaften haben, die in den klassischen Zwei-Partner-Situationen fehlten. In der Tat, Vorteile existieren im Falle eines Viel-Partner-Netzes, wie auch, wenn der Authentisierung gleiches Gewicht gegeben wird wie der Geheimhaltung oder gar größeres, wie es für moderne Verfahren zur Abwicklung finanzieller Transaktionen der Fall ist.

10.1 Symmetrische und asymmetrische Chiffrierverfahren

10.1.1 Symmetrische Verfahren (*private key methods*)

Der Schlüssel, den zwei Partner vereinbart haben, bestimmt bei den **symmetrischen** Chiffrierverfahren in einfacher Weise sowohl den Chiffrierschritt wie den Dechiffrierschritt. Die meisten bisher vorgestellten (vor dem Siegeszug der Elektronik benutzten) Verfahren sind in diesem Sinne symmetrische Verfahren. Für eine zweiseitige Nachrichtenverbindung benötigt dabei, wenn der Chiffrierschritt χ_{k_j} eineindeutig ist (2.6.2), jede Seite nur *einen* Chiffrier-und-Dechiffrier-Schlüssel, jede Seite aber einen anderen.

Auch bei dem in 9.6 diskutierten DES, dem wohl bekanntesten Vertreter moderner Blockchiffrierung, unterscheiden sich Chiffrier- und Dechiffrierschritt beispielsweise nur in der Reihenfolge, in der die aus dem Schlüssel generierten Teilchiffrierungen angewandt werden. Solche symmetrische Verfahren können heute durch sehr effiziente Algorithmen maschinell realisiert werden. Insbesondere durch Hardware-Lösungen in Form spezieller Chips waren 1995 bereits Durchsatzraten von mehr als 20 Mbits/s erreichbar.

Die Chiffriersicherheit beruht wesentlich auf der Geheimhaltung des Chiffrier-Schlüssels. Unter der Annahme, daß es für den Unbefugten selbst bei Kenntnis der Verfahrensklasse undurchführbar ist, diesen Schlüssel zu gewinnen, ist es unter realen Bedingungen weithin noch üblich, der Echtheit der Botschaften und der Identität des jeweiligen Gegenübers zu vertrauen (siehe jedoch 10.5). Authentisierung wird nicht als Problem gesehen und gilt naiverweise als garantiert, sobald und soweit Sicherheit garantiert ist.

Zu diesen Vorzügen gesellen sich natürlich auch einige Nachteile, die anwendungsabhängig mehr oder weniger stark ins Gewicht fallen:

(1) Es ist nicht möglich, Dritten gegenüber nachzuweisen, daß ein bestimmter Absender eine bestimmte Meldung geschickt hat. Diese fehlende rechtliche Sicherheit stellt insbesondere für die Übermittlung von Aufträgen und für finanzielle Transaktionen ein deutliches Manko dar.

(2) Die Schlüssel müssen vorher über einen hinreichend gesicherten Kanal vereinbart bzw. ausgetauscht werden. Eine spontane gesicherte Kommunikation ist nicht möglich.

(3) Ein weiteres Problem kann in der Anzahl der benötigten Schlüssel liegen. Bei n Partnern in einem Netz, wobei jeder mit jedem gesichert Daten austauschen möchte, sind $\binom{n}{2} = n \cdot (n-1)/2$ involutorische Schlüssel oder symmetrische Schlüsselpaare erforderlich. Bei $n = 1\,000$ ergibt dies immerhin bereits $499\,500$ Schlüssel.

10.1.2 Asymmetrische Chiffrierverfahren (*public key methods*)

Stellt man die Symmetrie der Chiffrierung aber einmal in Frage, nimmt man insbesondere an, daß sowohl zum Chiffrieren wie zum Dechiffrieren ein eigener Schlüssel benutzt wird, so erkennt man sofort, daß selbstverständlich der zur *Dechiffrierung* erforderliche Schlüssel absolut geschützt werden muß, daß aber der zur *Chiffrierung* erforderliche Schlüssel dem Gegner sogar bekannt sein darf. Man spricht dann von einem **asymmetrischen** Chiffrierverfahren.

Für eine zweiseitige Nachrichtenverbindung der Partner $\mathcal{A}$ und $\mathcal{B}$ unterscheidet man jetzt vier Schlüssel: den öffentlichen Schlüssel (*public key*) von $\mathcal{A}$, den $\mathcal{B}$ zur Chiffrierung benutzt, und den privaten Schlüssel (*private key*) von $\mathcal{A}$, den nur $\mathcal{A}$ kennt und den $\mathcal{A}$ zur Dechiffrierung benützt, wie auch den öffentlichen Schlüssel von $\mathcal{B}$ und den privaten von $\mathcal{B}$. Aber $\mathcal{A}$ kann jetzt Nachrichten von vielen Partnern erhalten, die alle für ihre Chiffrierung seinen öffentlichen Schlüssel kennen. Für ein Netz von n Partnern benötigt man deshalb nur noch n asymmetrische Schlüsselpaare, im Gegensatz zu $\binom{n}{2}$ symmetrischen Schlüsselpaaren.

Das Konzept der *public key*–Verfahren stammt von *Whitfield Diffie* und *Martin E. Hellman.*[1]

10.1.3 Asymmetrische Chiffrier- und Signatur-Verfahren

Wir betrachten nun folgende Situation: Der öffentliche Schlüssel KP_i des i-ten Teilnehmers bestimmt in einfacher Weise die Chiffriermethode E_i, die ihn erreichbar macht und einem Verzeichnis (*directory*) veröffentlicht wird, der private Schlüssel KC_i die Dechiffriermethode D_i, die tunlichst nur dem i-ten Teilnehmer und niemand sonst zugänglich ist. Genauer gesagt: E_i wie auch D_i sollen effiziente Realisierungen besitzen, aber für alle Teilnehmer ist es praktisch undurchführbar, d.h. aus Zeit- und Speichergründen zum Mißerfolg verdammt, KC_i aus KP_i herzuleiten.

---

[1] *New Directions in Cryptography*, Trans. IEEE Inform. Theory, IT-22, **6** (1976), 644–654.

Die folgende Eigenschaft von E_i und D_i

(*) $D_i(E_i(x)) = x$,

erlaubt ein der Geheimhaltung dienendes
asymmetrisches Chiffrierverfahren.

Die folgende *zusätzliche* Eigenschaft von E_i und D_i

(**) $E_i(D_i(x)) = x$,

erlaubt ein auch der Authentisierung dienendes
asymmetrisches Chiffrier- und Signaturverfahren.

Das asymmetrische Chiffrierverfahren arbeitet folgendermaßen:

Wenn Partner $\mathcal{A}$ einen Klartext m chiffriert an $\mathcal{B}$ senden will, nimmt er aus dem öffentlichen Verzeichnis unter dem Eintrag $\mathcal{B}$ den Schlüssel $KP_{\mathcal{B}}$ (der $E_{\mathcal{B}}$ festlegt), chiffriert m:

$(A) \qquad c = E_{\mathcal{B}}(m)$

und sendet den Geheimtext c über das öffentliche Netz an $\mathcal{B}$.

$\mathcal{B}$ benützt seinen privaten Schlüssel $KC_{\mathcal{B}}$ (der $D_{\mathcal{B}}$ festlegt),
um den Klartext m wiederzugewinnen:

$(B) \qquad D_{\mathcal{B}}(c) = D_{\mathcal{B}}(E_{\mathcal{B}}(m)) = m \qquad$ (wegen (*))

Das asymmetrische Chiffrier- und Signaturverfahren arbeitet wie folgt:

Wenn Partner $\mathcal{A}$ einen Klartext m mit seiner Unterschrift "A" signiert an $\mathcal{B}$ senden will, chiffriert er erst m mit seinem privaten Schlüssel $KC_{\mathcal{A}}$ (der $D_{\mathcal{A}}$ festlegt),

$(A1) \qquad d = D_{\mathcal{A}}(m)$,

und fügt zu d seine Unterschrift "A" im Klartext hinzu. Sodann nimmt er aus dem öffentlichen Verzeichnis unter dem Eintrag $\mathcal{B}$ den Schlüssel $KP_{\mathcal{B}}$ (der $E_{\mathcal{B}}$ festlegt) und chiffriert das Paar ("A", d):

$(A2) \qquad e = E_{\mathcal{B}}(\text{“}A\text{”}, d) = E_{\mathcal{B}}(\text{“}A\text{”}, D_{\mathcal{A}}(m))$.

$\mathcal{A}$ sendet den Geheimtext e über das öffentliche Netz an $\mathcal{B}$.

$\mathcal{B}$ benützt seinen privaten Schlüssel $KC_{\mathcal{B}}$ (der $D_{\mathcal{B}}$ festlegt),
um das Paar ("A", d) wiederzugewinnen:

$(B1) \qquad D_{\mathcal{B}}(e) = D_{\mathcal{B}}(E_{\mathcal{B}}(\text{“}A\text{”}, d)) = (\text{“}A\text{”}, d) \qquad$ (wegen (*)) .

$\mathcal{B}$ erkennt aus "A", daß $\mathcal{A}$ der Absender ist. $\mathcal{B}$ benützt jetzt den öffentlichen Schlüssel $KP_{\mathcal{A}}$ von $\mathcal{A}$ (der $E_{\mathcal{A}}$ festlegt), um aus d den Klartext m wiederzugewinnen:

$(B2) \qquad E_{\mathcal{A}}(d) = E_{\mathcal{A}}(D_{\mathcal{A}}(m)) = m \qquad$ (wegen (**)) .

Sofern $\mathcal{B}$ vernünftigen Text bekommt, kann er sicher sein, daß dieser von $\mathcal{A}$ stammt, da kein anderer Partner ihn mit $D_{\mathcal{A}}$ chiffriert haben könnte.

10.1.4 Asymmetrische Chiffrierverfahren weisen zwar die in 10.1.1 genannten Nachteile der symmetrischen Verfahren nicht auf. Es ergeben sich aber andere Probleme (s. 10.2.3, 10.4 und 10.6).

Moderne Varianten von Signaturverfahren unterwerfen den Klartext einem Einweg-*hash*-Algorithmus (siehe 10.5), signieren das Ergebnis und übertragen diese Signatur als Anhang. Sie sparen damit Zeit und vermeiden außerdem die Möglichkeit, den Klartext aus der Signatur zu rekonstruieren; allerdings kann das Zwischenschalten des *hash*-Algorithmus zu einer Schwachstelle der Authentisierung führen.

10.2 Einweg-Funktionen

KP_i zu einem *öffentlichen Schlüssel* zu machen, erfordert, daß es ‚praktisch undurchführbar' (engl. *intractable*) ist, $D_i = E_i^{-1}$ durch Funktionsumkehrung aus E_i zu erhalten (vgl. 8.9.2); daß also E_i eine ‚Einweg-Funktion' ist.

10.2.1 Echte Einweg-Funktionen

Eine injektive Funktion

$$f : X \to Y$$

heißt echte **Einweg-Funktion** (engl. *one way function*), falls folgendes gilt:

Es gibt ein effizientes[2] Verfahren zur Berechnung von $f(x)$ für alle $x \in X$,
Es gibt kein effizientes Verfahren zur Bestimmung von x aus der Beziehung $y = f(x)$ für alle $y \in f[X]$.

Arto Salomaa hat ein schlagendes Beispiel einer Einweg-Funktion gegeben. Eine Chiffrierung mit homophonen Chiffrierschritten $Z_{26} \dashrightarrow Z_{10}^7$ sei folgendermaßen definiert: Für einen Buchstaben X wird *irgendein* Name, der mit diesem Buchstaben beginnt, im Telefonbuch einer großen Stadt Y aufgesucht; eine 7-ziffrige Telefonnummer, die unter diesem Namen aufgeführt ist, wird als Ergebnis des Chiffrierschritts gewählt. Um ein Beispiel zu geben: Die Chiffrierung von /kindergarten/ könnte in folgenden Chiffrierschritten ablaufen

k	⊢⇢	Koch	⊢⇢	8202310	i	⊢⇢	Ivanisevic	⊢⇢	8119896
n	⊢⇢	Nadler	⊢⇢	6926286	d	⊢⇢	Dicklberger	⊢⇢	5702035
e	⊢⇢	Esau	⊢⇢	8348578	r	⊢⇢	Remy	⊢⇢	7256575
g	⊢⇢	Geith	⊢⇢	2730661	a	⊢⇢	Aranyi-Gabor	⊢⇢	2603760
r	⊢⇢	Rexroth	⊢⇢	5328563	t	⊢⇢	Tecins	⊢⇢	6703008
e	⊢⇢	Eisenhauer	⊢⇢	7913174	n	⊢⇢	Neunzig	⊢⇢	3002123

/kindergarten/ wird also chiffriert in eine Folge von 12 sieben-ziffrigen Codegruppen

8202310 8119896 6926286 5702035 8348578 7256575 2730661 2603760
5328565 6703008 7913174 3002123 ,

[2] Effizient: Mit einem Rechenaufwand, der polynomial ist in $\log |X|$. Wenn P = NP gelten würde, existierte keine echte Einwegfunktion.

dazu braucht ein menschlicher Chiffrierer weniger als eine Minute Zeit. Die Dechiffrierung ist eindeutig, erfordert aber Stunden und Stunden, wenn sie lediglich mit Hilfe des Telefonbuches von ungefähr 2 000 Seiten geschehen soll. Eine Einweg-Funktion stellt bereits für einen befugten Entzifferer fast unüberwindliche Schwierigkeiten dar.

Somit können echte Einweg-Funktion kaum zur Chiffrierung dienen. Einweg-Funktionen ohne Homophone können allerdings zur **Identifikation** und **Authentisierung** herangezogen werden: Zur Zugangskontrolle für Rechner wird ein Kennwort (‚Paßwort') durch eine echte Einweg-Funktion chiffriert und in dieser Form im Rechner gespeichert. Wann immer Zugriff verlangt wird, wird das vorgezeigte Paßwort ebenfalls chiffriert und die Kryptogramme werden verglichen. Ein eventueller Einblick in die gespeicherte Datei ist nutzlos. Dieses Verfahren wird in dem weitverbreiteten Betriebssystem UNIX[3] verwendet, gegründet jedoch auf eine Variante des DES-Algorithmus, der wohl nicht als echte Einweg-Funktion angesehen werden kann.

Zurück zu *Salomaas* Beispiel: Es ist jedoch denkbar, daß der befugte Entzifferer ein inverses Telefonbuch besitzt, wie es heute mehr oder weniger legal erhältlich ist. Ein solches Buch macht die Dechiffrierung so einfach wie die Chiffrierung. Es wirkt wie eine **Falltüre**, eine Geheimtüre, die in einer Richtung offensichtlich, in der anderen jedoch getarnt ist: Sie zu finden und zu öffnen kostet viel Zeit, außer man kennt die Lage des auslösenden Knopfes.

10.2.2 Einweg-Funktionen mit Falltüre

Zum Zwecke der Datensicherheit, die wesentlich kryptologischer Natur ist, werden Einweg-Funktionen mit Falltüre gebraucht, die dem authorisierten Benutzer die Dechiffrierung erlauben.

Eine injektive Funktion

$$f : X \to Y$$

heißt **Einweg-Funktion mit Falltüre** (engl. *trapdoor one way function*), falls folgendes gilt:

> Es gibt ein effizientes Verfahren zur Berechnung von $f(x)$ für alle $x \in X$,
> Es gibt ein effizientes Verfahren zur Berechnung von $f^{-1}(y)$ für alle $y \in f[X]$, aber für alle $y \in f[X]$ kann $f^{-1}(y)$ nicht effizient aus der Relation $y = f(x)$ berechnet werden: Dazu ist zusätzliche Information über das Öffnen einer Falltüre notwendig.

Die Falltüre in *Salomaas* Beispiel ist das inverse Telefonbuch. Es kann als einmalige Investition vom Chiffrierer, der die Zeit dazu aufbringt und es häufig genug zu gebrauchen gedenkt, legal hergestellt werden; der Speicherbedarf ist nicht größer als der für das originale Telefonbuch. Eine solche Art von Vorarbeit ist eine der besten Strategien zum Brechen asymmetrischer Chiffrierverfahren, da diese normalerweise für einige Zeit unverändert gebraucht werden.

---

[3] UNIX ist ein eingetragenes Warenzeichen.

10.2.3 Die Effizienzgrenze

Die Funktionsumkehrung scheitert bei Einweg-Funktionen – seien sie echt oder mit Falltüren, die man nicht kennt – nur am erforderlichen Aufwand an Rechenzeit und Speicherplatz, an ihrer Zeit- und Speicherkomplexität. Die Grenze zwischen 'effizient durchführbar' und 'praktisch undurchführbar' verschiebt sich wegen des technologischen Fortschritts zwar laufend: Grob gerechnet ist zur Zeit alle zwei Jahre eine Verdopplung der Rechenleistung zu beobachten, alle 15 Monate eine Halbierung der Kosten pro Speicherbit. Die niedrigen Preise für die Hardware ermöglichen eine massive Parallelisierung, die bei dieser Art von Aufgaben auch voll zu nutzen wäre. Der Kryptologe kann aber durch eine entsprechende Erhöhung der Parameterwerte rechtzeitig ‚gegensteuern' und eine Funktionsumkehrung für absehbare Zeit praktisch undurchführbar machen.

Ein Beispiel soll dies verdeutlichen: Bei einigen Verfahren läuft die Funktionsumkehrung einer Einweg-Funktion auf die Zerlegung einer Zahl n in ihre Primfaktoren hinaus. Das 'Quadratic Sieve'[4], ein schneller Algorithmus mit ‚subexponentieller Komplexität', benötigt dazu einen Aufwand, der asymptotisch von der Größenordnung

$$e^{\sqrt{\ln n \cdot \ln(\ln n)}} = n^{\sqrt{\ln(\ln n)/\ln n}}$$

Operationen ist. Für $n = 10^{70}$ hat der Exponent $\sqrt{\ln(\ln n)/\ln n}$ ungefähr den Wert 0.178, entsprechend ist $n^{\sqrt{\ln(\ln n)/\ln n}} = 2.69 \cdot 10^{12}$.

Zur Eichung mag dienen, daß 1984 auf einer CRAY X-MP die Faktorisierung von $(10^{71}-1)/9$ 9.5 Stunden dauerte; das ergibt rund $80 \cdot 10^6$ ‚Makro-Rechenschritte' pro Sekunde, und extrapoliert folgendes Bild (wobei alle zwei Jahre eine Verdopplung, alle zwanzig Jahre eine Vertausendfachung der *maximalen* Rechenleistung angenommen ist)

n	$e^{\sqrt{\ln n \cdot \ln(\ln n)}}$	Rechenzeit 1984	Rechenzeit 1994	Rechenzeit 2004
10^{50}	$1.42 \cdot 10^{10}$	181 sec	5.66 sec	181 msec
10^{70}	$2.69 \cdot 10^{12}$	9.5 h	0.297 h	34.2 sec
10^{100}	$2.34 \cdot 10^{15}$	344 Tage	10.75 Tage	8.3 h
10^{120}	$1.31 \cdot 10^{17}$	52.57 Jahre	600 Tage	19.3 Tage
10^{140}	$5.49 \cdot 10^{18}$	$2.2 \cdot 10^3$ Jahre	68.75 Jahre	803 Tage
10^{200}	$1.20 \cdot 10^{23}$	$4.8 \cdot 10^7$ Jahre	$1.5 \cdot 10^6$ Jahre	$4.8 \cdot 10^4$ Jahre
10^{280}	$1.12 \cdot 10^{28}$	$4.4 \cdot 10^{12}$ Jahre	$1.4 \cdot 10^{11}$ Jahre	$4.4 \cdot 10^9$ Jahre

Die **Effizienzgrenze** der ‚jahrelangen' Arbeit verschiebt sich also von (1984) $n = 10^{100} = 2^{332}$ über (1994) $n = 10^{120} = 2^{399}$ auf (2004) $n = 10^{140} = 2^{465}$. Aufsehen erregte 1994 die geglückte Zerlegung einer 129-stelligen Zahl (mit

[4] Aufbauend auf frühe Arbeiten von M. Kraitchik, verbessert von C. Pomerance (1985), P. Montgomery (1987), R. D. Silverman (1987). Die schnellste Version dieses Algorithmus ist als 'Double Large Prime Variation of the Multiple Polynomial Quadratic sieve' (ppmpqs) bekannt. Weder sie noch die noch bessere 'Number Field Sieve' Methode (NSF) von John Pollard (1988), die asymptotisch eine Anzahl Schritte von der Ordnung $e^{(\ln n)^{1/3} \cdot (\ln(\ln n))^{2/3}} = n^{(\ln(\ln n)/\ln n)^{2/3}}$ braucht, ist effizient im Sinne von 10.2.1 .

429 Bits) in ihre beiden je 65-stelligen Primfaktoren. Nach der obigen Extrapolation wären dazu auf einem Höchstleistungsrechner 3330 Tage erforderlich. Tatsächlich wurde die Gesamtarbeit auf 1600 über *Internet* verbundene, schwächere Computer verteilt und in 8 Monaten erledigt. 1999 wurde eine Zahl mit 465 Bits faktorisiert. Seit dem Jahr 2000 gibt es mit 512 Dualstellen keine Sicherheit mehr.

Auch wenn hochgradig parallelisierte Spezialrechner den Rechenzeitbedarf weiterhin verringern werden, es gibt Grenzen, die mit den bekannten Verfahren aus physikalischen Gründen wohl nie überschritten werden können. Zum Beispiel würde ein 10^{60}-Bit-Speicher mehr als die Masse unseres gesamten Sonnensystems benötigen, ebensowenig sind 10^{70} Operationen realisierbar, weil selbst bei einer der ‚Elementarlänge' von 10^{-15}m entsprechenden ‚Elementarzeit' von $\frac{1}{3} \cdot 10^{-23}$ sec pro ‚Makro-Rechenschritt' die dazu erforderliche Zeit die Lebensdauer des Sonnensystems bei weitem übersteigt.

Aber diese großen Zahlen können trügerisch sein. Es gibt keinen Beweis dafür, daß kein wesentlich schnellerer Algorithmus als das *Quadratic Sieve* und vergleichbare existiert. Es könnte ja sein, daß die Primfaktorzerlegung von n in einer Zeitspanne getan werden kann, die nur polynomial mit n ansteigt. Aber es ist nicht sehr glaubhaft. Häufig findet sich der gefühlsmäßige Einwand, daß man für die Primfaktorzerlegung mehr als zweitausend Jahre Zeit hatte, um sich etwas einfallen zu lassen.

Allgemein ist die Nichtexistenz von Falltüren anscheinend nur schwer beweisbar. Und die Komplexitätstheorie in ihrem derzeitigen Zustand liefert meist nur obere Schranken für den Aufwand: “*There are no provable lower bounds for the amount of work of a cryptanalyst analyzing a public-key cryptosystem*” (Salomaa 1990). Eine neue Falltüre wie auch ein schnellerer Algorithmus für die Funktionsumkehrung der Einweg-Funktion würde die Sicherheit des Chiffrierverfahrens ebenso in Frage stellen wie ein direkter Entzifferungsangriff, der die Funktionsumkehrung vollständig umgeht. Hierin liegt *prinzipiell* eine große Gefahr für die asymmetrischen Verfahren.

10.2.4 Bekannte Verfahren

Man kann im übrigen schwer beweisen, daß es Einweg-Funktionen überhaupt gibt, da bei den bekannten Verfahren hinlänglich gute untere Schranken im strengen Sinn fehlen. Wir haben aber gute *Kandidaten*, die auf den folgenden beiden Operationen basieren: Multiplikation ganzer Zahlen und Exponentiation über dem endlichen Körper $\mathbb{F}(p)$, p prim.

10.2.4.1 Einweg-Funktion ohne Falltür: Multiplikation von Primzahlen

Es ist, wie *Turing* schon 1937 bemerkte (5.7), vergleichsweise einfach, zwei zehntausendstellige ganze Zahlen und damit auch eine Anzahl von Primzahlen solcher Länge miteinander zu multiplizieren; es ist aber – siehe oben – heute kein effizientes Verfahren (öffentlich) bekannt, eine 160-stellige Dezimalzahl in ihre Primfaktoren zu zerlegen (von Sonderfällen abgesehen).

Die injektive Funktion

$f : X \to \mathbb{N}$ definiert durch $f(x_1, x_2) = x_1 \cdot x_2$

mit $X = \{(x_1, x_2) \mid x_1,\, x_2$ Primzahlen , $K \le x_1 \le x_2\}$

kann deshalb für hinreichend großes K (vgl. 10.2.3) als Kandidat für eine Einweg-Funktion betrachtet werden. Es sind keine Falltüren bekannt.

10.2.4.2 Einweg-Funktion ohne Falltür: Exponentiation in $\mathbb{F}(p)$.

Es sei p eine Primzahl. Für festes a kann die a-Exponentialfunktion

$F_a : \mathbb{Z}_{p-1} \to \mathbb{Z}_p \backslash \{0\}$ definiert durch $F_a(n) = a^n \mod p$

für hinreichend große p und a als Kandidat für eine Einweg-Funktion in Betracht gezogen werden (für $\mathbb{Z}_p$ s. Kap. 5).

Beispiel: $p = 7$, $\mathbb{Z}_p \backslash \{0\} = \{1, 2, 3, 4, 5, 6\}$, $a = 2$:

n	0	1	2	3	4	5	6
2^n	1	2	4	8	16	32	64
$2^n \bmod 7$	1	2	4	1	2	4	1

Der Berechnungsaufwand für F_a hält sich selbst für 10^{160} überschreitende Werte von p, a in erträglichen Grenzen. Die schon in 9.5.2 aufgetretene grundlegende Idee des fortgesetzten Quadrierens und Multiplizierens gemäß der Dualdarstellung des Exponenten zeigt folgendes Beispiel:

$$a^{25} = \left(\left(\left(a^2 \cdot a\right)^2\right)^2\right)^2 \cdot a \,, \quad \text{da} \quad 25 = \mathbf{LLOOL} \,.$$

Dabei wird nach jeder Quadrierung und nach jeder Multiplikation eine Reduktion *modulo p* durchgeführt.

Das Beispiel $a = 2$, $p = 7$ zeigt daß die a-Exponentialfunktion F_a nicht notwendigerweise injektiv ist. Wenn jedoch F_a injektiv ist über $\mathbb{Z}_p \backslash \{0\}$ und somit ein Gruppenisomorphismus von $\mathbb{Z}_{p-1}$ und $\mathbb{Z}_p \backslash \{0\}$, dann wird a eine **Primitivwurzel** (‚primitive Kongruenzwurzel') genannt, wie etwa $a = 3$, $a = 11$, $a = 13$, $a = 17$ für $p = 31$:

3^n mod 31 ergibt eine Permutation mit der (13+9+8)-Zyklenzerlegung

(1 3 27 23 11 13 24 2 9 29 21 15 30) (6 16 28 7 17 22 14 10 25) (4 19 12 8 20 5 26 18)

11^n mod 31 ergibt eine Permutation mit der (26+3+1)-Zyklenzerlegung

(1 11 24 8 19 22 18 2 28 10 5 6 4 9 23 12 16 20 25 26 7 13 21 27 15 30) (3 29 17) (14)

12^n mod 31 ergibt eine zyklische Permutation mit dem Zyklus

(1 12 20 23 28 26 2 24 9 15 25 21 4 17 18 30 19 11 8 3 5 29 7 22 16 6 10 27 14 13)

13^n mod 31 ergibt eine Permutation mit der (13+6+6+4+1)-Zyklenzerlegung

(1 13 11 3 27 23 24 2 14 19 21 15 30) (4 10 5 6 16 18) (7 22 9 29 12 8) (20 25 26 28) (17)

Man kann zeigen, daß es für jede Primzahl p mindestens eine Primitivwurzel gibt. In der Tat ist ihre Anzahl $\varphi(p-1)$ (für die Eulersche Funktion φ siehe 5.6), weitere für $p = 31$ sind 17, 21, 22, 24 ($\varphi(30) = 8$). Für spezielle p mag es Besonderheiten geben. Beispielsweise sind für 5, 17, 257, 65537 und für

alle größeren Primzahlen der Form $p = 2^{2^k} + 1$ (Fermatsche Primzahlen) — wenn es solche gibt — 3 und 7 stets Primitivwurzeln (*Albert H. Beiler*, *Armin Leutbecher*).

Wenn nun a eine primitive Kongruenzwurzel ist, hat F_a eine Inverse F_a^{-1}, genannt die **diskrete a-Logarithmus-Funktion** oder der **Index** in $\mathbb{Z}_p \backslash \{0\}$. Während zwar die Exponentiation *modulo* p vergleichsweise schnell durchführbar ist, ist es schwer einen effizienten Algorithmus für die Berechnung des diskreten Logarithmus zu finden.

Unter den bekanntgewordenen Algorithmen für den diskreten Logarithmus über einer multiplikativen Gruppe wie etwa $\mathbb{Z}_p \backslash \{0\}$ erfordern selbst gute wie der *Giant-Step-Baby-Step* Algorithmus[5] (*D. Shanks 1971*) einen Aufwand proportional $\sqrt{|Z_p|} = \sqrt{p} = e^{\frac{1}{2}\ln p}$ und sind damit nicht effizient.

Die besseren *Index Calculus* Methoden — die das Aufstellen einer geeigneten Basis für die multiplikative Gruppe, gewöhnlich die ersten t Primzahlen erfordern und damit die Vorausberechnung einer riesigen Datenbasis — funktionieren nur in günstig gelagerten Fällen, haben jedoch immer noch subexponentielle Komplexität, d.h. sie brauchen einen Aufwand der gleichen Größenordnung $e^{\sqrt{\ln p \cdot \ln(\ln p)}}$ wie die Primfaktorzerlegung durch das *Quadratic Sieve*.

$(\mathbb{Z}_p, +, \times)$ ist ein endlicher Körper, ein sogenanntes Galoisfeld $\mathbb{F}(p)$ der Characteristik p. Allgemeiner betrachtet man das Galoisfeld $\mathbb{F}(p^k)$, eine Körpererweiterung von $\mathbb{F}(p)$, und seine multiplikative Gruppe $\mathbb{F}(p^k)\backslash\{0\}$, die weiterhin eine zyklische Gruppe ist. Sie wird erzeugt durch irgendein Element x, das eine nichttriviale Wurzel der Gleichung $x^{p^k} - x = 0$ ist. Die Elemente von $\mathbb{F}(p^k)$ sind dann die p^k Polynome vom Höchstgrad $k-1$ über dem Galoisfeld $\mathbb{F}(p)$ und können implementiert werden als ein k-dimensionaler Vectorraum.

Beispiel: $p = 2$, $k = 3$, $\mathbb{F}(2^3) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$. $x^8 - x$ hat einen irreduziblen Faktor $x^3 + x + 1$, Potenzen werden durch $x^3 \mapsto x + 1$ reduziert.

Es ist die multiplikative Gruppe von $\mathbb{F}(p^k)\backslash\{0\}$, die eine tragende Rolle spielt. Für $k > 1$ ist diese Multiplikation verschieden von der der modularen Arithmetik. Somit haben wir schließlich den Gruppenisomorphismus

$$F_a : \mathbb{Z}_{p^k-1} \to \mathbb{F}(p^k)\backslash\{0\} \quad \text{definiert durch} \quad F_a(n) = a^n \text{ in } \mathbb{F}(p^k)$$

Im Beispiel $\mathbb{F}(2^3)$ mit $a = x$ und mit $a = x+1$:

n	0	1	2	3	4	5	6	7
x^n	1	x	x^2	x^3	x^4	x^5	x^6	x^7
x^n red.	1	x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1

n	0	1	2	3	4	5	6	7
$(x+1)^n$	1	$x+1$	$(x+1)^2$	$(x+1)^3$	$(x+1)^4$	$(x+1)^5$	$(x+1)^6$	$(x+1)^7$
$(x+1)^n$ red.	1	$x+1$	x^2+1	x^2	x^2+x+1	x	x^2+x	1

[5] Für ein lauffähiges Program siehe Otto Forster, *Algorithmische Zahlentheorie*, Vieweg, Braunschweig 1996.

Der Fall $p=2$ bei großem k ist von besonderem Interesse. 1988 hat John Pollard eine Variante *Number Field Sieve* (NSF) der *Index Calculus* Methode angegeben, wobei die Primzahlen durch irreduzible Polynome ersetzt werden – mit einer durch $e^{((\ln p)^{1/3} \cdot (\ln \ln p)^{2/3})}$ bestimmten Komplexität. Mit massiver Parallelberechnung hat man Vorarbeiten für so anspruchsvolle Probleme wie $\mathbb{F}(2^{503})$ bewältigt (*Coppersmith* 1986, *McCurley* 1990, *Gordon* und *McCurley* 1993).

Ein natürlicher nächster Schritt im Gebrauch von Gruppenisomorphismen wurde durch die Methode der elliptischen Kurven (*elliptic curve method*, ECM), entwickelt von *Neil Koblitz* (1985), *V. S. Miller* (1985), *Hendrik W. Lenstra, jr.* (1986) getan. Die Methode greift den Gebrauch gewisser algebraischer Kurven dritter Ordnung in der projektiven Ebene über einem Körper K auf, und zwar speziell über $\mathbb{F}(p^k)$. Einige Algorithmen wie der *Giant-Step-Baby-Step* Algorithmus können auf die Punktgruppe einer diskreten elliptischen Kurve übertragen werden. Es hat den Anschein, daß für die sonst ziemlich gute *Index Calculus* Methode das Finden einer Basis im Falle elliptischer Kurven wenig aussichtsreich ist. Somit verspricht die *Index Calculus* Methode unter Gebrauch elliptischer Kurven möglicherweise größere Sicherheit für Identifikation und Authentisierung, was sie derzeit zu einem interessanten Gegenstand der Forschung macht. Elliptische Kurven über $\mathbb{F}(2^k)$ (Fall $p = 2$) sind besonders vorteilhaft, da arithmetische Prozessoren für den zugrundeliegenden Körper leicht zu konstruieren und für große k vergleichsweise einfach zu implementieren sind.

Für die bisher betrachteten Methoden sind keine Falltüren bekannt geworden, auch nicht für den Fall $\mathbb{F}(2^k)$, $k > 1$. Für nicht aus Primzahlpotenzen zusammengesetztes q hat $F_a(x) = a^x \mod q$ eine Falltüre, wenn q ein Produkt von zwei Primzahlen ist – nach Faktorzerlegung von q ist der Chinesische Restesatz anwendbar zur Erstellung einer Tafel, die die Berechnung erleichtert.

10.2.4.3 Einweg-Funktion mit Falltür: h-te Potenz *modulo* q

In (9.5.2) wurde die Potenzierung eingeschränkt auf den Körper $\mathbb{F}(p)$. Nun mag q auch zusammengesetzt sein; der Exponent h sei eine feste natürliche Zahl,

$$P_h(x) = x^h \mod q .$$

Es gibt immer noch geeignete Paare (h, h') fester Zahlen aus $\mathbb{Z}_q \backslash \{0\}$ (für $q=10$ vgl. Tabelle 1 (5.5) mit $N=4$: $h \cdot h' \equiv 1 \mod 4$) derart, daß

(1) ein effizientes Verfahren existiert, $P_h(x)$ für alle $x \in \mathbb{Z}_q$ zu berechnen,

(2) ein effizientes Verfahren existiert, $P'_h(x)$ für alle $x \in \mathbb{Z}_q$ zu berechnen,

wobei $P_{h'}(P_h(x)) = x$ und $P_h(P_{h'}(x)) = x$.

Aber: Es ist – falls nur h und q bekannt sind und etwa $q > 10^{200}$ gilt – kein effizienter Algorithmus zur Bestimmung der h-ten Wurzel *modulo* q (öffentlich) bekannt.

Es gibt jedoch eine *Falltüre:* Ein solcher Algorithmus kann viel leichter angegeben werden, wenn q Produkt zweier großer Primzahlen ist und die Zerlegung von q in Primfaktoren bekannt ist (s. 10.3).

10.2.4.4 Einweg-Funktion mit Falltür: Quadrierung *modulo* $q = p' \cdot p''$

Hier handelt es sich um den wichtigen Sonderfall $h = 2$ von 10.2.4.3. Es geht um ‚quadratische Reste', Quadratwurzeln *modulo* q , mit denen sich schon *Legendre* und *Gauß* beschäftigten. Eine Anwendung für öffentliche Chiffriersysteme wurde 1985 von *H. C. Williams* untersucht.

Wir betrachten zunächst den Fall $q = p$, p prim. Tabelle 1 (5.5) zeigt für ungerades p unter $N = p-1$ keine Einträge für $h = 2$. P_2 ist weder injektiv noch surjektiv. Für die zweideutige (doppelsinnige) Umkehrung von P_2 schreiben wir $\sqrt{\ }$. Durch Umkehrung der Funktionstabelle erhält man etwa für $p = 17$

$\sqrt{1} = \pm 1$ $\sqrt{2} = \pm 6$ $\sqrt{4} = \pm 2$ $\sqrt{8} = \pm 5$ $\sqrt{9} = \pm 3$ $\sqrt{13} = \pm 8$ $\sqrt{15} = \pm 7$ $\sqrt{16} = \pm 4$.

Für p prim gibt es effiziente Verfahren zur Berechnung der Quadratwurzel, die auf dem Gaußschen Reziprozitätsgesetz für quadratische Reste aufbauen.

Anders für zusammengesetzte q, etwa $q = p' \cdot p''$: Wenn erst die Faktorisierung von q bekannt ist, kann man, wenn man Quadratwurzeln $\pm u$ von a *modulo* p' und Quadratwurzeln $\pm v$ von a *modulo* p'' , $u \neq v$, bereits kennt, $\sqrt{a}$ *modulo* q leicht berechnen. Sonst aber ist nach *M. O. Rabin* (1979) die Umkehrung jedenfalls ebenso schwierig wie die Faktorisierung von q.

10.3 RSA-Verfahren

Dieses wohl bekannteste Verfahren[6] ist nach seinen Entwicklern *Ronald L. Rivest, Adi Shamir, Leonard M. Adleman* (1978) benannt, der Patentschutz in den U.S.A. reicht bis 20. September 2000. Es beruht auf der (weithin akzeptierten) Vermutung, daß die Potenzierung *modulo* q unter bestimmten Voraussetzungen eine Einweg-Funktion mit Falltüre ist (s. 10.2.2 und 10.2.4.3). Anders als in 9.5.2 ist q nicht prim.

10.3.1 Für den i-ten Partner in einem asymmetrischen Chiffrierverfahren sei

(1) $q_i = p'_i \cdot p''_i$, wo p'_i , p''_i ungerade Primzahlen sind, $p'_i \neq p''_i$.

(2) $e_i\,,\ d_i \in \{1, 2, \ldots, \psi(q_i) - 1\} \subset \mathbb{Z}_{q_i} \backslash \{0\}$, mit

(2a) $\mathrm{ggt}\,(e_i, \psi(q_i)) = 1$, (2b) $\mathrm{ggt}\,(d_i, \psi(q_i)) = 1$,

(2c) $e_i \cdot d_i \bmod \psi(q_i) = 1$,

wo ψ die Carmichael-Funktion bezeichnet,[7]

$$\psi(p'_i \cdot p''_i) = \mathrm{kgv}\,(p'_i - 1\,, p''_i - 1) = 2 \cdot \mathrm{kgv}\,(\tfrac{p'_i - 1}{2}\,, \tfrac{p''_i - 1}{2})\ .^{8}$$

---

[6] US Patent 4 405 829 vom 20. September 1983.

[7] Im Originalverfahren wird an Stelle der Carmichaelschen Funktion die Eulersche φ-Funktion verwendet. Die angegebenen Bedingungen gewährleisten die Bedingungen des Originalverfahrens.

[8] Es gilt $\psi(2 \cdot p'_i \cdot p''_i) = \mathrm{kgv}(1\,, p'_i - 1\,, p''_i - 1) = \mathrm{kgv}(p'_i - 1\,, p''_i - 1)$.

Das RSA-Verfahren ist eine hochgradig polygraphische, monoalphabetische Blockchiffrierung mit Klartextzeichen $p_j \in \mathbb{Z}_{q_i}$ und Chiffrenzeichen $c_j \in \mathbb{Z}_{q_i}$; der Klartext wird gegebenenfalls vor der Anwendung des Verfahrens geeignet zerlegt und auf eine Folge von Elementen aus $\mathbb{Z}_{q_i}$ abgebildet.

Es werden folgende Schlüssel für den i-ten Partner verwendet:

öffentlich: e_i (normalerweise zum Chiffrieren)[9] , q_i,

privat: d_i (normalerweise zum Dechiffrieren)

Der Chiffrierschritt ist über die Einweg-Funktion $E_i : \mathbb{Z}_{q_i} \to \mathbb{Z}_{q_i}$ definiert:

$$E_i(m) = m^{e_i} \bmod q_i = c_i \ .$$

Der Dechiffrierschritt ist durch die Funktion $D_i : \mathbb{Z}_{q_i} \to \mathbb{Z}_{q_i}$ gegeben:

$$D_i(c) = c^{d_i} \bmod q_i = m_i \ .$$

Daraus resultiert ein asymmetrisches Chiffrier- und Signatursystem, da

$$D_i(E_i(x)) = E_i(D_i(x)) = x \text{ für alle } x \in \mathbb{Z}_{q_i} \ .$$

Der Beweis geht im wesentlichen wie in 9.7.2. Man kann ihn auf folgendes Korollar des Satzes von *Carmichael* für teilerfremde a , n stützen:

$$\text{Wenn } b \equiv b' \bmod \psi(n) \text{ , so } a^b \equiv a^{b'} \bmod n \ .$$

10.3.2 Beispiele

Auf *Salomaa* zurück geht folgendes Beispiel:

$$(e_i\,,\,d_i) = (1031\,,\,31\,963\,885\,304\,131\,991)$$
$$q_i = 32\,954\,765\,761\,773\,295\,963 = 3\,336\,670\,033 \cdot 9\,876\,543\,211\,;$$
$$\psi(q_i) = 16\,477\,382\,874\,280\,041\,360\ .$$

Sogar ein Beispiel mit derart großen Zahlen ist unrealistisch für praktische Sicherheit. Zu Demonstrationszwecken verwenden wir hinfort Beispiele mit kleinen Zahlen, die sich mit einem Taschenrechner nachrechnen lassen.

Beim Entwurf eines RSA-Chiffrierverfahrens geht man zweckmäßigerweise von der Falltür-Information aus: wir beginnen deshalb mit zwei Primzahlen

$$p_i' = 47\ ,\ p_i'' = 59\ .$$

Daraus ergibt sich:

$$q_i = p_i' \cdot p_i'' = 47 \cdot 59 = 2773\ ,\ \ \mathbb{Z}_{q_i} = \mathbb{Z}_{2773} = \{0\,,\,1\,,\,2\,,\,\ldots\,,\,2772\}\ ,$$
$$\psi(q_i) = \psi(2773) = kgv\,(46\,,\,58) = 1334\ .$$

Für die allgemeine Definition von $\psi(n)$ siehe etwa *Scholz-Schoeneberg*, Einführung in die Zahlentheorie, de Gruyter, 5. Aufl., Berlin 1973. $\psi(n)$ ist Teiler von $\varphi(n)$, wo φ die Eulersche Funktion ist. Der Satz von *Robert D. Carmichael* (1879–1967) besagt: Für teilerfremde a, n gilt $a^{\psi(n)} \bmod n = 1$, und zwar ist $\psi(n)$ der kleinste Exponent x derart, daß $a^x \bmod n = 1$ für alle zu n teilerfremden a gilt.
Der Satz von *Carmichael* ist *"... a very useful, but often forgotten, generalization of Euler's theorem"* (*H. Riesel*, Prime Numbers and Computer Methods for Factorization. Birkhäuser, Basel 1985). Tatsächlich erwähnen *Rivest, Shamir, Adleman* ihn nicht und auch *Salomaa* weist 1990 noch nicht auf ihn hin. *Scholz-Schoeneberg* geben *Carmichael* als Quelle nicht an.

[9] Da $2 \mid \psi(p_i' \cdot p_i'')$, ist $e_i = 2$ ausgeschlossen.

Nun muß e_i so festgelegt werden, daß $\mathrm{ggt}(e_i, 1334) = 1$ gilt. Es gibt viele Möglichkeiten, wie $e_i = 3, 5, 7, \ldots, 19, 21, 25, 27, 33, 35, 37, 39, \ldots$ – wenn eine Menge $\{e_i^{(j)}\}$ ausgewählt wird, ist sogar polyalphabetische Chiffrierung möglich.

Wir wählen[10] $e_i = 17$. Man erhält d_i mit dem schnellen Divisionsalgorithmus (vgl. 9.5.1): aus der Bedingung $e_i \cdot d_i \equiv 1 \mod 1334$ ergibt sich $d_i = 157$.

Chiffriert wird also mittels

$$E(m) = m^{17} \mod 2773 .$$

Wegen $17 = \mathbf{LOOOL}$ kann dieser Schritt durch

$$\left(\left(\left((m^2 \mod 2773)^2 \mod 2773\right)^2 \mod 2773\right)^2 \mod 2773\right) \cdot m \mod 2773$$

effizient realisiert werden.

Dechiffriert wird – ebenso effizient – mit Hilfe von

$$D(c) = c^{157} \mod 2773 .$$

Codiert man die Zeichen ␣ (Zwischenraum)[11], A, B, ..., Z als 00, 01, 02, ..., 26, so können wegen $2626 < 2773$ jeweils Blöcke von zwei aufeinanderfolgenden Zeichen in einem Schritt chiffriert werden.

Die Nachricht

errare␣humanum␣est

wird also zunächst als

05 18 18 01 18 05 00 08 21 13 01 14 21 13 00 05 19 20

codiert und anschließend (blockweise) chiffriert:

1787 2003 2423 0596 0340 1684 0340 0508 2109 .

Identische Klartextblöcke führen bei dieser Chiffrierweise zu identischen Geheimtextblöcken – die Chiffrierung ist blockweise monoalphabetisch. Dieser ECB-Modus (in DES-Sprechweise, 9.6.3) könnte in der Praxis – um die Kryptanalyse zu erschweren – durch einen CBC-artigen Modus ersetzt werden. Aber sogar periodische polyalphabetische Chiffrierung wäre vorzuziehen.

10.4 Anmerkungen zur Sicherheit von RSA

Neben den klassischen kryptanalytischen Ansätzen (s. Teil II), die man jedenfalls versuchen soll, gibt es bei dem RSA-Verfahren spezifische weitere:

---

[10] d_i soll dabei nicht zu klein ausfallen, damit es nicht durch einfaches Probieren herausgefunden werden kann. Es ist also besser, d_i zu wählen und e_i zu bestimmen.

[11] Entgegen der klassischen Gepflogenheit haben *Rivest, Shamir und Adleman* den Zwischenraum nicht unterdrückt. Die Literatur über das RSA-Verfahren folgt ihnen darin.

10.4.1 Angriff durch Faktorisierung von q_i

Gelingt es dem unbefugten Entzifferer, die Zerlegung $q_i = p_i' \cdot p_i''$ zu finden, so kann er $\psi(q_i) = 2 \cdot \text{kgv}\,(\frac{p_i'-1}{2}, \frac{p_i''-1}{2})$ berechnen und mit der Kenntnis von e_i nach 10.3.1 (2c) leicht auch d_i berechnen.

Um das RSA-Verfahren gegen diesen Angriff abzusichern, das heißt, die Faktorisierung von q_i praktisch undurchführbar zu machen (die tatsächliche Faktorisierung erfordert häufig mehr Aufwand als der Nachweis der Faktorisierbarkeit), sollten folgende Bedingungen erfüllt sein:

(1) $q_i = p_i' \cdot p_i'' > 10^{160}$.

(2) p_i' und p_i'' (als Dezimalzahlen) unterscheiden sich in ihrer Länge um etliche Stellen.

(3) Weder p_i' noch p_i'' sind klein, oder sind aus einer Primzahltafel genommen, oder sind von spezieller Form.

Die Bedingung (1) ist nach 10.2.1 verständlich. Die Bedingung (2) vereitelt die exhaustive Suche nach einer Darstellung von q_i als Differenz von Quadraten:

$$q_i = p_i' \cdot p_i'' = \left(\tfrac{p_i'+p_i''}{2}\right)^2 - \left(\tfrac{p_i'-p_i''}{2}\right)^2$$

mit ab $\sqrt{q_i}$ laufenden Werten für $\frac{p_i'+p_i''}{2}$. Die Bedingung (3) vereitelt die exhaustive Suche in einer relativ kleinen Menge von Primzahlen.

Der Aufwand für die Bestimmung von Primzahlen, die (1), (2) und (3) genügen, ist vergleichsweise gering. Von keinem dieser Angriffe wurde bisher berichtet, daß er erfolgreich gewesen wäre, vermutlich weil diese Sicherheitsvorschriften relativ leicht einzuhalten sind.

10.4.2 Angriff durch Iteration (vgl. 9.4.2)

Es sei

$c^{(0)} = m_j$ (Klartextblock) ,

$c^{(1)} = c_j = E_i(m_j) \bmod q_i$ (Geheimtextblock) .

Man wiederholt

$c^{(\kappa+1)} = E_i(c^{(\kappa)}) \bmod q_i \; (i = 1, 2, 3, \ldots)$.

Das kleinste $k \geq 1$ mit $c^{(k+1)} = c^{(1)}$ ist die Ordnung s_{m_j} von m_j ; s_{m_j} gibt die Länge des Zyklus an, in dem sich m_j befindet. $s_{m_j} - 1$ heißt **Wiederherstellungsexponent** (engl. *recovery exponent*) von m_j .

Beispiel 1: Wie oben, mit $m_j = 0518$

$(e_i, d_i) = (17, 157)$ $q_i = 47 \cdot 59 = 2773$; $\psi(q_i) = 2668 = 2^2 \cdot 23 \cdot 29$

$c^{(0)} = m_j$	$= 0518$	$(= 11 \cdot 47 + 1)$
$c^{(1)} = c_j$	$= 0518^{17} \bmod 2773 = 1787$	$(= 38 \cdot 47 + 1)$
$c^{(2)}$	$= 1787^{17} \bmod 2773 = 0894$	$(= 19 \cdot 47 + 1)$
$c^{(3)}$	$= 0894^{17} \bmod 2773 = 1364$	$(= 29 \cdot 47 + 1)$
$c^{(4)}$	$= 1364^{17} \bmod 2773 = 0518 = m_j$	

Hier sind wir wieder beim Klartext angelangt! Der Wiederherstellungsexponent von m_j ist also gleich 3. Dem unbefugten Dechiffrierer wird dies spätestens bei der nächsten Iteration klar:

$$c^{(5)} = 0518^{17} \mod 2773 = 1787 = c_j \ .$$

Es gilt nach dem Korollar des Satzes von *Carmichael* (10.3.1):

$$c^{(k)} = m^{17^k} \mod 2773 = m_j^{17^k \mod 1334} \mod 2773 \ .$$

Es ist jedoch $17^{44} \mod 1334 = 1$; deshalb $c^{(44)} = m_j^1 \mod 2773 = m_j$. 44 ist also eine obere Schranke für die längste mit $e = 17$ auftretende Periode. Beachte, daß 44 Teiler ist von $\psi(\psi(2773)) = \psi(\psi(47 \cdot 59)) = \psi(2 \cdot 23 \cdot 29) = 2 \cdot 11 \cdot 14 = 308$. Tatsächlich gibt es

9 Zyklen der Länge 1 (Fixpunkte)
42 Zyklen der Länge 4 – darunter der obige Zyklus von 0518
6 Zyklen der Länge 22
56 Zyklen der Länge 44 .

Beispiel 2:

$$(e_i\,,\,d_i) = (7\,,\,23) \qquad q_i = 55 = 5 \cdot 11\ ; \qquad \psi(q_i) = 20 = 2 \cdot 2 \cdot 5\ .$$

Dieses Beispiel ist klein genug, daß man alle Zyklen auflisten kann:

9 Zyklen der Länge 1 (Fixpunkte):

(0) (1) (10) (11) (21) (34) (44) (45) (54)

3 Zyklen der Länge 2:

(12, 23) (22, 33) (32, 43)

10 Zyklen der Länge 4:

(2, 18, 17, 8) (3, 42, 48, 27) (4, 49, 14, 9) (5, 25, 20, 15) (6, 41, 46, 51)
(7, 28, 32, 13) (16, 36, 31, 26) (19, 24, 29, 39) (30, 35, 40, 50) (37, 38, 47, 53)

Es ist $7^4 \mod 20 = 1$. Eine obere Schranke für die längste mit $e_i = 7$ auftretende Periode ist 4. Beachte, daß 4 übereinstimmt mit

$$\psi(\psi(55)) = \psi(20) = 4\ .$$

Beispiel 3:

$$(e_i\,,\,d_i) = (3\,,\,675) \qquad q_i = 1081 = 23 \cdot 47\ ; \qquad \psi(1081) = 506 = 2 \cdot 11 \cdot 23\ .$$

Es ist $3^{55} \mod 506 = 1$. 55 ist also eine obere Schranke für die längste mit irgendeinem e_i auftretende Periode. Beachte, daß 55 die Hälfte ist von

$$\psi(\psi(1081)) = \psi(506) = 2 \cdot 5 \cdot 11\ .$$

Ein solcher Zyklus der Länge 55 ist

(512, 768, 430, 531, 629, 98, 722, 683, 209, 284, 995, 653, 16, 853,
813, 535, 239, 1051, 25, 491, 190, 55, 982, 439, 54, 719, 676, 568,
393, 307, 397, 331, 384, 324, 721, 1041, 860, 1005, 991, 675, 213, 538,
660, 807, 606, 627, 101, 108, 347, 192, 581, 354, 867, 2, 8).

Es gibt typischerweise 16 Zyklen der Länge 55, 12 Zyklen der Länge 11, 12 Zyklen der Länge 5 und wiederum 9 Zyklen der Länge 1 (Fixpunkte)[12]: (0) (1) (46) (47) (93) (988) (1034) (1035) (1080).

Um das RSA-Verfahren auch gegen diesen Angriff abzusichern, das heißt einen großen Wiederherstellungsexponenten für hinreichend viele $m \in Z_{q_i}$ zu erreichen, sollte $\psi(\psi(q_i))$ möglichst groß sein. Es gilt nämlich:

> Die Periode – der Iterationsexponent – ist für alle e_i, die teilerfremd zu $\psi(q_i)$ sind, ein Teiler von $\psi(\psi(q_i))$; diese Schranke kann sogar (für geeignete e_i) erreicht werden.

Der Beweis stützt sich auf das Korollar des Satzes von *Carmichael*:

$$c^{(k)} = m_j^{e_i^k} \bmod q_i = (m_j^{e_i^k \bmod \psi(q_i)}) \bmod q_i$$
$$= (m_j^{(e_i^k \bmod \psi(\psi(q_i))) \bmod \psi(q_i)}) \bmod q_i ;$$

mit $k = \psi(\psi(q_i))$ ergibt sich

$$c^{(\psi(\psi(q_i)))} = m_j^{e_i^{\psi(\psi(q_i))}} \bmod q_i = (m_j^{e_i^0 \bmod \psi(q_i)}) \bmod q_i = m_j^1 \bmod q_i = c^{(0)} .$$

Somit ist $\psi(\psi(q_i))$ eine Periode und ein Vielfaches des Iterationsexponenten.

Um wenigstens $\psi(q_i') = \psi(p_i' \cdot p_i'') = 2 \cdot \text{kgv}\,(\frac{p_i'-1}{2}, \frac{p_i''-1}{2})$ möglichst groß zu haben, sollten folgende Bedingungen für die Wahl von p_i' und p_i'' erfüllt sein

(4) $p_i' - 1$ und $p_i'' - 1$ enthalten große Primfaktoren,

(5) $\text{ggt}\,(p_i' - 1 , p_i'' - 1)$ ist sehr klein.

Die Bedingungen (4) und (5) sind in idealer Weise erfüllt, wenn p_i', p_i'' sichere Primzahlen (9.5.2) sind. Dann sind sowohl $\frac{p_i'-1}{2}$ wie auch $\frac{p_i''-1}{2}$ prim, $\psi(q_i) = 2 \cdot \frac{p_i'-1}{2} \cdot \frac{p_i''-1}{2} \approx q_i/2$.

Der Aufwand, sichere Primzahlen zu finden, mag sich lohnen; es ist im übrigen nicht bewiesen, daß unendlich viele sichere Primzahlen existieren.

Überdies zu verhindern, daß $\psi(\psi(q_i))$ klein wird, bedeutet angesichts von $\psi(2 \cdot \frac{p_i'-1}{2} \cdot \frac{p_i''-1}{2}) = 2 \cdot \text{kgv}\,((\frac{p_i'-1}{2} - 1)/2, (\frac{p_i''-1}{2} - 1)/2) = 2 \cdot \text{kgv}\,(\frac{p_i'-3}{4}, \frac{p_i''-3}{4})$ daß für p_i' und p_i'' auch die folgenden Bedingungen gelten sollten:

(6) $\frac{p_i'-3}{4}$ und $\frac{p_i''-3}{4}$ enthalten große Primfaktoren,

(7) $\text{ggt}\,(\frac{p_i'-3}{4}, \frac{p_i''-3}{4})$ ist sehr klein.

Die Bedingungen (6) und (7) sind in idealer Weise erfüllt, wenn zusätzlich $\frac{p_i'-1}{2}$ and $\frac{p_i''-1}{2}$ sichere Primzahlen sind, d.h., p_i' und p_i'' **doppelt sichere Primzahlen** sind; dann sind $\frac{p_i'-3}{4}$ und $\frac{p_i''-3}{4}$ prim, $\psi(\psi(q_i)) = 2 \cdot \frac{p_i'-3}{4} \cdot \frac{p_i''-3}{4}$.

---

[12] Fixpunkte können nicht völlig vermieden werden: *Salomaa* hat gezeigt, daß es stets mindestens neun Fixpunkte gibt.

Doppelt sichere Primzahlen sind 11, 23, 47, 167, 359, 719, 1439, 2039, 2879, 4079, 4127, 4919, 5639, 5807, 5927, 6047, 7247, 7559, 7607, 7727, 9839, 10799, 11279, 13799, 13967, 14159, 15287, 15647, 20327, 21599, 21767, ... ; auch 2 684 999, 5 369 999, und 10 739 999.

Abgesehen von 11, sind alle doppelt sicheren Primzahlen von der Form $24a - 1$. Für doppelt sichere Primzahlen p_i', p_i'' (vgl. Beispiel 3) ergibt sich $\psi(\psi(q_i)) \approx q_i/8$.

10.4.3 Angriff bei kleinem e_i

Der Arbeitsaufwand zur Chiffrierung ist klein, wenn e_i klein ist – im Extremfall $e_i = 3$. Das mag zu bedenken sein, wenn der Sender nur über beschränkte Mittel verfügt – z.B. eine Chipkarte, und wenn der Empfänger von einem ziemlich großen d_i nicht erdrückt wird, etwa weil er einen zentralen Rechner verfügbar hat.

Kleine d_i sollten ohnehin nicht verwendet werden, um einen exhaustiven Angriff auszuschließen. Aber kleine e_i zu verwenden ist ebenfalls gefährlich: Wenn dann ein und die selbe Nachricht mit den Blöcken m_j (ein Rundschreiben) an viele verschiedene Empfänger verschickt wird unter Verwendung der selben Potenz $e_1 = e_2 = \ldots = e_s = e$ und mit verschiedenen (vermutlich paarweise teilerfremden) $q_1, q_2, \ldots q_s$ chiffriert wird, mit Chiffraten $m_j^e \bmod q_1$, $m_j^e \bmod q_2, \ldots, m_j^e \bmod q_s$, so läßt sich *modulo* $q_1 \cdot q_2 \cdot \ldots \cdot q_s$ der Wert von $m' = m^e$ mit Hilfe des Chinesischen Restesatzes berechnen. Dann gilt jedoch $m_j^e = m'$, und diese Gleichung mit bekanntem m' und bekanntem kleinem e läßt sich, obschon große Zahlen involviert sind, leicht nach m_j lösen.[13] Der Einbruch ist jedoch noch nicht komplett: d_i muß noch bestimmt werden.

10.4.4 Nicht nur sollten beim RSA-Verfahren gewisse Klartextblöcke vermieden werden, die zu sehr kleinen Wiederherstellungsexponenten führen können. Beispiel 2 zeigt, daß auch eine unbedachte Wahl von e_i die maximale Zyklenlänge vermindern kann. Gewisse Möglichkeiten für e_i sollten vollständig vermieden werden: $e_i = \psi(q_i) + 1$ bewirkt, daß $d_i = \psi(q_i) + 1$ wird und damit $E_i(m_j) = D_i(m_j)$ zur identischen Abbildung entarten.

10.4.5 Das RSA-Verfahren gilt weithin als praktisch sicher, sofern obige Bedingungen erfüllt sind; zumindest sind keine ernsthaften erfolgreichen Angriffe öffentlich bekannt geworden.

Das Verfahren hat aber auch seine Nachteile:

RSA erfordert relativ lange Schlüssel, in naher Zukunft 1024 oder mehr Bits.

RSA ist im Vergleich zu DES etwa um den Faktor 1 000 langsamer.

---

[13] *M. J. Wiener*, *Cryptanalysis of short RSA secret exponents.* EUROCRYPT '89 Proceedings. Lecture Notes in Computer Science 434, Springer 1990.
Auch: IEEE Transactions on Information Theory, Vol. 36 No. 3, May 1990, pp. 553–558.

10.5 Geheimhaltung versus Authentisierung

Ein öffentlicher Chiffrier-Schlüssel weist auf ein Problem hin, das die klassische Kryptographie vernachlässigt: Sie glaubt, sie habe es nur mit dem passiven Gegner zu tun, der chiffrierte Nachrichten, die über Draht, elektromagnetische Wellen oder akustisch übermittelt werden, mitliest oder abhört (engl. *eavesdropping*), um die Chiffrierung zu brechen; im übrigen nimmt sie mit Gelassenheit an, daß es dem Gegner noch schwerer als dies fallen würde, eine Nachricht mit dem eigenen Schlüssel zu chiffrieren und aktiv in das eigene Netz einzuschmuggeln oder als solche auszugeben. Dies ist fahrlässig.

Wenn Funkkontakt mit Spionen gehalten wurde, zeigte sich indes das Problem auf seiner menschlichen Seite: Ein Spion konnte gefangengenommen werden, und selbst wenn es nicht gelang ihn „umzudrehen", konnte sein Funkgerät von jemand anderem benutzt werden. Ein solches ‚Funkspiel' fand 1942–1943 zwischen Deutschen und Engländern statt, wobei ein niederländischer Untergrundagent verwickelt war. Stets eine Unterschrift des Funkers zu verlangen, nützt nichts, wenn dieser umgedreht wurde und dann bedeutete es auch nichts, daß man seine ‚Handschrift' kannte. Wenn er jedoch unter Gewaltandrohung zur Kollaboration gezwungen worden war, gelang es ihm vielleicht, die ‚security checks', die er unregelmäßig zur Authentisierung einzustreuen hatte — gewisse eigentümliche Rhythmen, die er sonst nicht gebrauchte — zu unterlassen oder zu ändern, ohne daß er Verdacht erregte. Man sicherte sich also in einer Weise, wie es im zivilen Verkehr durch die unverwechselbaren Eigenheiten der Unterschriften geschieht.

Die Verwendung öffentlicher Schlüssel bietet nun einem Betrüger geradezu an, sich in eine Nachrichtenverbindung einzuschleichen. Die Authentisierung wird ebenso wichtig wie die klassische Geheimhaltung. In Geheimdiensten ist Authentisierung mit Geheimhaltung gleichrangig.

Jedoch besteht zwischen diesen beiden Grundsätzen ein tiefer Konflikt, wie das folgende Beispiel zeigt: Handelt es sich um eine Nachricht mit Alarmcharakter, so kann man sie speichern und später wieder einschleusen; dadurch kann man falschen Alarm auslösen. Dagegen kann man sich durch eine Zeitangabe in der Nachricht schützen – muß allerdings dabei eine Klartext-Geheimtext-Kompromittierung (11.1.2) in Kauf nehmen. Es zeigt sich also, daß Geheimhaltung und Authentisierung getrennte Dinge sind, die sich nicht nur gegenseitig nicht nach sich ziehen, sondern sogar behindern.

Überdies kann man feststellen, daß eine Chiffrierung gegen Brechen umso besser geschützt ist, je weniger Redundanz sie enthält; gegen Fälschung dagegen, umso mehr Redundanz sie enthält (man kann das am Banknotendruck studierern). Geheimhaltung einerseits, Authentisierung andrerseits sind also einander widersprechende Aufgaben; um beiden zu genügen, sind zwei voneinander unabhängige Anstrengungen erforderlich.

Chiffrierverfahren, die nach 10.1.3 sogar Signaturverfahren sind, ermöglichen einen guten Kompromiß: Zusätzliche identifizierende Information nach verabredeten Protokollen und vorab fehlererkennende (4.4.6) Codierung.

Asymmetrische Verfahren haben sogar ihre besondere Stärke bei der Authentisierung, sie werden ferner (darauf haben *Diffie* und *Hellman* von Anfang an nachdrücklich hingewiesen) besonders vorteilhaft auch beim Schlüsselaustausch eingesetzt: Da Signaturen wie auch Schlüssel verhältnismäßig kurz sind gegenüber Nachrichten, kann der größere Zeitaufwand, den die hochrangigen asymmetrischen Verfahren erfordern (er kann um ein Vielfaches größer sein), eher in Kauf genommen werden. Verfahren mit öffentlichen Schlüsseln sind keine Alternative zu klassischen symmetrischen Verfahren, sie ergänzen sich gegenseitig. Im Zahlungsverkehr werden heute in der Regel die Daten nur schwach chiffriert, der Authentisierung wird jedoch verständlicherweise die größte Aufmerksamkeit geschenkt, sie wird auch entsprechend gut bezahlt.

Der 1992 publizierte *Digital Signature Standard* (DSS) des N.I.S.T. (National Institute of Standards and Technology) der U.S.A. beruht auf dem *Digital Signature Algorithmus* (DSA), der, auf Patenten von *Schnorr* und *ElGamal* aufbauend, die diskrete Logarithmusfunktion (10.2.4.2) benutzt. Er hat sich umfangreiche Kritik gefallen lassen müssen; insbesondere wurde bemängelt, daß nicht das RSA-Verfahren genormt wurde.

Zur sender- und empfängerseitigen Bildung von 160-Bit-Prüfgruppen ('*message digest*') dient der standardisierte *Secure Hash Algorithm* des N.I.S.T..

Im übrigen ist es auch wichtig, Vergabe und Verwaltung öffentlicher Schlüssel einer vertrauenswürdigen Instanz zu übertragen. Eine solche zu finden ist ein politisches Problem; eine Behörde, zu deren Aufgabe auch Kryptanalyse gehört, wird es schwer haben, in der Öffentlichkeit als unvoreingenommen zu gelten.

10.6 Sicherheit der öffentlichen Chiffrierverfahren

Wie schon einleitend gesagt, wird bei den bisher vorgeschlagenen Verfahren mit öffentlichen Schlüsseln (*public cryptography*) zur Chiffrierung kommerzieller Nachrichtenwege *Shannon*s Maxime im Extrem befolgt: *Die Sicherheit beruht allein auf dem Dechiffrierschlüssel.* Dies allerdings geschieht nicht nur aus kryptographischen Gründen; hier wird eine Not zur Tugend gemacht.[14] Mit der Öffentlichkeit der Kryptographie wird nun auch die Kryptanalyse in den öffentlichen Bereich gerückt. Die Öffentlichkeit könnte den Eindruck gewinnen, daß auch die Kryptanalyse mehr denn je öffentlich ist.

Dem ist nicht so: Sie ist weiterhin geheimnisvoll. Trotzdem muß man feststellen, daß die öffentlich verwendeten Verfahren beim professionellen Kryptanalytiker reine Freude hervorrufen müssen. Neben den systembedingten

[14] Mittlerweile auch bei symmetrischen Verfahren, bei denen es gar nicht nötig wäre.

Angriffswegen liegen alle klassischen Angriffswege offen, insbesondere wird bei heftigem Verkehr ein- und derselbe fortlaufende Schlüssel häufig wiederholt angewandt. Auch muß man sich vor schlauen Ideen besonders hüten. Beispielsweise könnte die Verwendung von doppelt sicheren Primzahlen eine *complication illusoire* sein: Vielleicht bieten sie gerade einen Angriffsweg zur Reduktion der Exhaustion.[15]

Was jedoch dem zivilen, kommerziellen Benutzer trügerische Sicherheit vorspiegelt, ist die rein kombinatorische Komplexität. Abhandlungen, in denen die Komplexität der Verfahren berechnet wird, unterstützen den beruhigenden Eindruck. Dabei ist es für den heutigen Zustand der Komplexitätstheorie bezeichnend, daß sie meist nur obere Schranken liefert – von unteren Schranken etwa für den Aufwand zur Primfaktorisierung scheinen die bekannten Verfahren noch weit entfernt zu sein (10.2.3). Der völlige Wegfall des Kryptosekretärs, sein Ersatz durch einen Computer macht die Sache im übrigen noch schlimmer: Zwar werden Chiffrier-Irrtümer wegfallen, aber auch der wachsame Verstand eines Menschen, der allein hilft, schwerwiegendere Chiffrierfehler zu vermeiden.

Somit darf man nicht erwarten, daß die vorgeschlagenen Chiffrierverfahren der *public cryptography* für Experten, insbesondere in den hoheitlichen Diensten, unangreifbar sind. Die Professionellen sind jedoch natürlicherweise sehr zurückhaltend und brüsten sich nicht mit ihren Fähigkeiten; eher neigen sie zur Untertreibung.

---

[15] Nach *A. Gerold* kann man aus dem Modul auf die Struktur der Primfaktoren schließen.

11 Chiffriersicherheit

"Even in cryptology, silence is golden."
Laurence D. Smith

Kennwörter dienen der Auswahl eines Verfahrens aus einer Verfahrensklasse, Schlüssel vor allem der Auswahl von Chiffrierschritten aus einem Chiffriersystem. Pessimistischerweise ist anzunehmen, daß der Gegner (engl. *adversary*, frz. *adversaire*) oder Feind (engl. *enemy*, frz. *ennemi*) die Verfahrensklasse kennt — es gibt ja nicht allzuviele, die im Gebrauch sind. Dem von *Kerckhoffs* formulierten ‚Grundgesetz der Kryptologie': ≪*Il faut qu'il puisse sans inconvénient tomber entre les mains de l'ennemi*≫ gab *Shannon* die Fassung "*The enemy knows the system being used*".

Daraus folgt zunächst, daß die Sicherheit weitgehend am Schlüssel hängt, und daß man mit der Wahl eines Schlüssels besonders vorsichtig zu sein hat. Der Gebrauch naheliegender Wörter ist trivialerweise ein schwerer Chiffrierfehler. Schon *Porta* hat darauf nachdrücklich hingewiesen: „Je mehr die Schlüsselwörter entfernt sind von gewöhnlicher Kenntnis, desto größere Sicherheit gewähren sie dem Schreiben". Dementsprechend gelangen auch schon unbefugte Entzifferungen durch Erraten des Schlüsselwortes, kaum daß der Gebrauch von Schlüsselwörtern aufkam. *Porta* schrieb, er habe einmal eine Nachricht innerhalb weniger Minuten gebrochen — er erriet den Schlüssel *OMNIA VINCIT AMOR*. *Giovanni Batista Argenti* hatte ebenfalls Glück, er erriet den Schlüssel *IN PRINCIPIO ERAT VERBUM*. Hehre Wörter wie *KAISER* und *VATERLAND*, *TORCH* und *LIBERTY*, *GLOIRE* und *PATRIE*, die hohe patriotische Gefühle ausdrücken, mögen sich zur Unterstützung der psychologischen Kriegsführung eignen, aber nicht als Schlüssel.[1]

11.1 Chiffrierfehler

Als **Chiffrierfehler** bezeichnet man Verstöße gegen die Chiffriersicherheit, also nicht nur den Gebrauch eines zu naheliegenden Schlüssels, sondern alles, was dem unbefugten Entzifferer die Arbeit leicht macht.

[1] Es ist erstaunlich, wie viele Leute heute als Rechnerzugangs-Paßwörter ihren Namen oder ihr Geburtsdatum verwenden — etwas anderes können sie sich nicht merken.

„Funken ist Landesverrat“ soll (nach *Praun*) Generalmajor *Erich Fellgiebel*, Chef des Wehrmacht-Nachrichtenverbindungswesens, zu Kriegsbeginn überdeutlich gesagt haben. In der Tat laden Funkverbindungen zum Abhören geradezu ein. Sie sollten also nur gebraucht werden, wenn alle anderen, sicheren Nachrichtenwege erschöpft oder unerreichbar sind. Während sich das disziplinierte Heer daran hielt und auch die Kriegsmarine, obschon sie auf See keine Drahtverbindungen benutzen konnte, galt Funken bei der Luftwaffe als Regelfall (*J. Rohwer*). „Görings bekannter Übermut ... konnte auch zu übermäßiger 'Lust zu funken', zu jeweils detaillierten Berichterstattungen, die sich nicht nur auf Luftkampfsituationen, sondern auch auf die Lage der Heeresverbände bezogen, führen“ (*R. Elble*). Unzulängliche Führungstechniken bestimmten den Geist des Göringschen Luftwaffenoberkommandos.

Über solche Kardinalfehler hinaus, gibt es viele Möglichkeiten, die Chiffriersicherheit zu verletzen.

11.1.1 Dazu gehören auch Irrtümer beim Chiffrieren. Sie machen zunächst dem *befugten* Dechiffrierer die Arbeit schwer oder ganz unmöglich. Im letzteren Fall steht das Unheil schon vor der Tür; die Nachricht muß nochmals angefordert werden. Wird nun die selbe Nachricht mit dem selben Schlüssel nochmals chiffriert (diesmal korrekt), so erlaubt der Vergleich der beiden, in der Regel bis auf die Stelle des Irrtums oder doch wenigstens bis zu dieser Stelle hin übereinstimmenden Nachrichten (‚Klartext-Klartext-Kompromittierung‘) durch eine ‚Differentialanalyse‘ gewisse Einblicke in das Verfahren. Wird jedoch mit der selben Nachricht ein anderer Schlüssel benutzt, so hat man die Situation einer ‚Geheimtext-Geheimtext-Kompromittierung‘, die mit geeigneten Methoden gelegentlich die Entzifferung des Schlüssels erlaubt – und zwar auch, wenn ein progressiver Schlüssel verwendet wurde, dessen Alphabete noch gar nicht wiederholt wurden. Unglaublicherweise wurde von den Deutschen im 2. Weltkrieg häufig der gleiche Befehl an Einheiten, die verschiedenen ‚Kenngruppen-Netzen‘ angehörten, in verschiedenen Chiffrierungen – bei auffällig gleicher Länge – gefunkt (*Heinz Ulbricht*: „Mitteilung von *Dönitz* auf vielen Schlüsseln, daß er zum Admiral befördert worden war“). Einzige Abhilfe ist: die Nachricht vollständig neu zu formulieren, unter Gebrauch anderer Wörter. Auch das russische Verfahren (3.4), die Nachricht ungefähr in der Mitte zu zerschneiden und verkehrt herum zmmenzusetzen, bietet keine Sicherheit.

11.1.2 Ein klassischer Kunstfehler ist es, wenn eine chiffrierte Nachricht nochmals, beispielsweise wegen Problemen des Schlüsselnachschubs, im Klartext übermittelt wird (‚Klartext-Geheimtext-Kompromittierung‘). Jetzt ist aus Klartext und Geheimtext nicht nur die Verfahrensklasse, sondern im Falle einer Shannonschen Chiffrierung (2.6.4) auch der Schlüssel rekonstruierbar. Damit wird möglicherweise nicht nur ein täglich wechselnder Schlüssel aufgedeckt, sondern auch ein darunter liegendes festes oder doch nur selten wechselndes Verfahren, etwa ein Codebuch. Deshalb gehörte „Weh dem der lügt und Klartext funkt“ zu den eisernen Regeln des in 4.4 erwähnten Leut-

nants *Jäger*, des Lieblings der alliierten kryptanalytischen Büros. Verständlich, daß es zu den Höhepunkten eines professionellen Kryptanalytikers zu gehören scheint, eine Klartext-Geheimtext-Kompromittierung zu erleben.

Verständlich auch, daß mit List und Schläue die Dienste versuchen, so etwas herbeizuführen. Da gelang es 1941 einem hohen japanischen Beamten, dem amerikanischen Botschafter *Joseph C. Grew* ein Papier zuzustecken mit der Bemerkung, daß ein Mitglied der japanischen Regierung der U.S. Regierung eine Botschaft übermitteln wolle, aber Angst habe, die Militärs könnten davon erfahren, und daß er sie deshalb im geheimsten diplomatischen Code übermitteln sollte. Der Angriff war gegen das Streifengerät M-138-A (vgl. 7.5.3) gerichtet, und so chiffriert ging die Nachricht in den Äther. Angeblich soll es den Japanern trotzdem nicht gelungen sein, M-138-A zu brechen.

Eine ähnliche Geschichte stammt aus der Zeit der Dreyfus-Affäre: Als 1894 *Alfred Dreyfus* auf ganz vage Anschuldigungen hin verhaftet worden war und *La Libre Parole* freudig das Ereignis hinausposaunt hatte, sandte Oberst *Panizzardi*, der italienische Militärattaché am Quai d'Orsay, ein Telegramm nach Rom. Die französischen Kryptanalysten, die eine Kopie erhielten, hatten Anlaß zu vermuten, daß ein kommerzieller (!) Code von *Baravelli* (4.4.3) benutzt worden war, der mit Einer-, Zweier-, Dreier- und Vierergruppen arbeitete, und daß dieser Code überschlüsselt war. Nach dem Teiltext /dreyfus/ suchend, der als 227 1 98 306 chiffriert sein mußte, fanden sie das Muster 527 3 88 706 und wußten, daß die Überschlüsselung nur die erste Ziffer berührte (es handelte sich um eine Umnumerierung der Seiten im Codebuch). Die Nachricht konnte bis auf die letzten vier Gruppen entziffert werden; über deren Bedeutung war man sich zunächst nicht im klaren. Man vermutete "*uffiziale rimane prevenuto emissaria*" und dies wurde (von *Sandherr*, dem Nachrichtendienst-Chef) als Beweis von *Dreyfus'* Schuld angesehen. Am nächsten Tag fand man das System der Überschlüsselung heraus, es ergab sich "*uffizialmente evidare commenti stampa*". Das entlastete *Dreyfus*, aber *Sandherr* meinte, „diese Dinge sind immer etwas unpräzise". Da kam *Matton*, ein Untergebener *Sandherrs*, auf die Idee, *Panizzardi* ein Telegramm unterzuschieben. Ein Doppelagent schleuste eine als wichtig aufgemachte Nachricht ein, und *Panizzardi* gab sie, wie sich herausstellte, fast wörtlich weiter. Die Kryptanalytiker, die nicht eingeweiht waren, lösten die Nachricht unmittelbar und *Matton* konnte sich von der Richtigkeit überzeugen. Dennoch wurde vor Gericht eine gefälschte Version verbreitet, und es dauerte bis 1906, bis *Dreyfus* rehabilitiert, d.h. von einem Gericht freigesprochen war. Die Affäre Dreyfus ist in Frankreich immer noch nicht ausgestanden: Im Februar 1994 enthob der französische Verteidigungsminister *François Léotard* den Leiter der historischen Abteilung der Landstreitkräfte, Oberst *Paul Gaujac*, wegen einer nicht genehmen „tendenziösen Analyse" des Falles Dreyfus seines Postens.

Auch Österreich-Ungarn hatte seinen Triumph: Als *Figl*s Leute 150 Wörter eines zwischen Rom und Konstantinopel benutzten italienischen diplomatischen Codes erforscht hatten, erweiterten sie ihr Wissen Schritt für Schritt,

indem sie Bruchstücke militärisch relevanter Informationen in eine italienischsprachige Zeitung in Konstantinopel schmuggelten. Innerhalb eines Monats konnten sie das ihnen bekannte Vokabular auf 2 000 Wörter erweitern.

Noch einfacher ist die Methode, für die die Russen berühmt sind: dem Botschafter den Klartext zu stehlen. In diesem Fall beeilt sich der Diplomat, seiner Regierung zu versichern, es sei kein Code der höchsten Geheimhaltungsstufe verwendet und dadurch bloßgestellt worden – auch wenn es nicht so ist. Selbst Italien hatte seine professionelle *squadra penetrazione*.

Ein Beispiel für einen überholten Code ist der GRAY-Code des *State Department*: Als er nach dem Ende des 1. Weltkriegs aufgestellt wurde, um die veralteten und kompromittierten Codes RED, BLUE, GREEN abzulösen, war wohl nicht damit gerechnet worden, daß er zwei Jahrzehnte in Gebrauch bleiben würde. Er war den *foreign service officers* so vertraut, daß Diplomaten Abschiedsreden in GRAY aus dem Stegreif halten konnten. *Roosevelt* sandte am 6. Dezember 1941 eine Notiz an *Cordell Hull*: "*Dear Cordell — Shoot this to Grew [der amerikanische Botschafter in Tokio] — I think can go in gray code — saves time — I don't mind if it gets picked up. FDR*". *Franklin Delano* erzielte nicht den gewünschten Effekt: Die Entzifferung dauerte Zeit und die persönliche Friedensbotschaft, die er dem Tenno übermittelte, kam zu spät – sie hätte wohl auch nichts mehr bewirkt.

11.1.3 Diese Episoden beleuchten eine allgemeine Methode der Kryptanalyse, die Methode des wahrscheinlichen Wortes. Solche Wörter sind oft durch aktuelle Ereignisse bestimmt. Sie müssen dann umschrieben werden. Französische Truppen führten im 1. Weltkrieg Angriffe gegen die deutschen Stellungen lediglich, um im deutschen Funkverkehr gewisse ‚wahrscheinliche Wörter' auszulösen – wie gut, daß Soldaten selten wissen, wofür sie kämpfen[2]. Neben Wörtern wie Angriff/*attack*/*attaque*, Bombardierung/*bombardment*/*bombardement* etc. aus aktuellen Anlässen birgt die militärische Sprache einen reichen Schatz auffälliger Wörter und stereotyper Phrasen wie ‚Hauptquartier' und ‚Generalkommando', ‚Divisionsstab' und ‚Radiostation'. Verheerend wirkt der alltäglich abgesetzte gleiche Spruch „Ohne besondere Vorkommnisse" oder „Nichts zu melden". An ihnen setzt die Methode des wahrscheinlichen Wortes ebenso an wie an den Wörtern Liebe, Herz, Feuer, Flamme, brennen, Leben, Tod, die schon *Porta* aufzählte als unabänderliche Requisiten von Liebesbriefen. Besonders gefährlich wird die Gewohnheit, stereotype Wendungen zu verwenden, im Hinblick auf den Wechsel des Schlüssels: Der neue Schlüssel kann aus den alten Phrasen unschwer binnen kurzem deduziert werden. Nicht immer wird man allerdings so viel Glück haben wie der Leutnant *Berthold* im Büro G.2 A.6 der *American Expeditionary Force* von 1918, der am 11. März 1918, 07:40 einen Funkspruch

[2] Die Briten ließen im 2. Weltkrieg eines ihrer Flugzeuge eine Leuchttonne, die eine Fahrrinne der sonst verminten Einfahrt nach Calais markierte, versenken – lediglich um den Spruch „Erloschen ist Leuchttonne" auszulösen, und auf /leuchttonne/ eine Suche anzusetzen (s. 14.1).

in Ziffern auffing – offenbar in einem neuen Schlüssel; und einige Stunden später einen Spruch gleicher Länge mit Buchstaben im alten Schlüssel – der Empfänger hatte die neuen Chiffrierunterlagen noch nicht vorliegen und um nochmalige Übermittlung im alten Schlüssel gebeten.

Auch beim PLAYFAIR-Handschlüssel des Deutschen Afrika-Korps passierte anläßlich einer Umstellung am 1. 1. 1942 eine solche Geheimtext-Geheimtext-Kompromittierung des Schlüssels.

Sehr folgenreich war eine Bloßstellung der noch nicht einmal eingesetzten 4-Rotor-ENIGMA Ende 1941 durch einige übungshalber parallel mit der 3-Rotor-ENIGMA chiffrierte Funksprüche. Bletchley Park war damit in der Lage, die Verdrahtung des neuen Rotors (der „Griechenwalze" β) herauszufinden, bevor am 1. Februar 1942 die 4-Rotor-ENIGMA offiziell eingeführt wurde.

Schon in Friedenszeiten muß ja das Handwerk gelernt werden: Weil man nichts Besseres weiß, werden in Manövern Standardtexte bekanntester Art, Sprichwörter, Redensarten übertragen. Bei genügender Einfallslosigkeit kann das eine Chiffrierung vollständig offenlegen, bevor noch der erste Schuß gefallen ist. Dazu schreibt *Hüttenhain*: „Es ist ein Fehler, ein Verfahren, das längere Zeit in einem kleinen Kreis bereits benutzt wurde, zum Hauptverfahren zu machen". Was die unter Umständen unvermeidbaren stereotypen Briefanfänge und -endungen (*"For Murphy"*, 4.4) anbelangt, hilft auch die oben erwähnte Methode des russischen Kopulierens nur wenig, sie sollte aber trotzdem verwendet werden, um unerfahrene Codebrecher irrezuführen.

11.1.4 Schließlich ist auch bereits das bloße Einsetzen des Funkverkehrs ein bedeutsames Zeichen.[3] Wenn man es sich leisten kann, sollte man Nachrichtenverbindungen kontinuierlich betreiben und auch in den Betriebspausen Text senden – keine Testsätze, keinen Zeitungstext, sondern irrelevanten, unperiodischen, am besten reinen Zufallstext oder synthetische Sprache, die möglichst auch die Häufigkeitscharakteristik der betreffenden Sprache zeigt, verwenden (‚Verkehrsauffüllung', engl. *traffic padding*). Durch zufallsbestimmten unregelmäßigen Neubeginn kann man aus einem Text von 10 000 Wörtern lange unperiodische synthetische Texte ableiten. Eine bessere, zur Herstellung synthetischer Sprache geeignete Methode hat *Küpfmüller* um 1950 angegeben. Aus einer Textvorlage wird eine n-gramm-Approximation durch einen Schieberegisterprozeß gewonnen: Für jeweils $n-1$ Zeichen wird im Text das nächste Vorkommnis gesucht und das darauffolgende Zeichen angehängt, das vorderste Zeichen entfernt und der Prozeß wiederholt. Mit einer Tetragramm-Näherung erhält man aus dem ersten Kapitel einer berühmten Novelle von *Thomas Mann* den folgenden Nonsense-Text, demgegenüber selbst *Helmut Heissenbüttel* bläßlich wirkt:

---

[3] Da während einer größeren militärischen Operation die Nachrichtenverbindungen erfahrungsgemäß stark belastet sind, pflegen die Stäbe einige Tage vor Beginn solcher Operationen regen persönlichen Verkehr (engl. *underwear effect* genannt).

thomas ist daher mit mein hand zeigen augen von geschaeftig
im kreissigenmauemdisellschaeftwar zur seligen durchterlich
hier familie hierheben herzigkeit mit eindrinnen tonyzu
plaudertfuenf uhr erzaehlung ich regeshaehm die konnte
neigte sie dern ich was stuetzte heissgetuebrige wahrend tause

Durch solches Verstecken der Nachricht in einem Wust belanglosen Textes wird die Arbeitslast, die der unbefugte Entzifferer aufzubringen hat, auf ein Vielfaches gesteigert und, vgl. 2.1.1, die erforderliche Verzögerung erreicht. Jedoch besteht das Problem, daß die Empfangsstelle höllisch aufpassen muß, um nicht ein eingeschobenes Stück echter Nachricht zu übersehen.

11.1.5 Selbst das Auffüllen mit stereotypen Blendern wie /x/, die Wiederholung ein und des selben Wortes oder die Verdoppelung von Buchstaben kann gefährlich sein. Abhilfe bringt Umschreibung, der Gebrauch von Synonyma oder die (wahllose!) Verwendung von Homophonen – hierzu gehört aber der Gebrauch von echten Blendern, um Teil-Wiederholungen in der Umgebung von Homophonen zu überdecken. Geradezu haarsträubend ist es, wenn in der Wehrmacht (Heer) für die aus gutem Grund fehlenden Interpunktionszeichen[4] ein /x/ (Punkt), /y/ (Komma) oder gar /xx/ (Doppelpunkt), /yy/ (Bindestrich), /j/ (Anführungszeichen) zu benutzen vorgeschrieben bzw. üblich war; dazu kam die Verdoppelung wichtiger Wörter oder Buchstaben wie /anan/, /vonvon/, auch Buchstabenverdreifachung: /bduuu/ für ‚Befehlshaber der U-Boote', /okmmm/ für ‚Oberkommando der Marine' (vgl. 9.2.5)[5]. Dies, zusammen mit unvermeidlichen Phrasen wie ‚auf Befehl des Führers', ‚Heil Hitler', die niemand zu unterdrücken wagte, half den Briten enorm, die ENIGMA zu brechen. Sie waren so an diese Dummheiten der Deutschen, etwa einen Spruch durch viele /x/ am Anfang und am Ende aufzufüllen, gewöhnt, daß sie sich sehr entrüstet zeigten, wenn ENIGMA-Entzifferungen unsinnige Texte (im britischen Jargon *quatsch* genannt) als Anfang und Ende ergaben.

Zu Zeiten der *Argentis* herrschte diesbezüglich mehr Aufmerksamkeit als im 19. und 20. Jahrhundert, wo man von der Unbrechbarkeit von überschlüsselten Codes und anderen kombinierten Verfahren übersteigerte Vorstellungen hatte. Das Weglassen von Buchstabenverdoppelungen ist nur eine Maßnahme unter den ‚absichtlichen Buchstabierfehlern', die schon die *Argentis* empfahlen. Zu Recht schrieb *Porta* schon 1563 „Denn es ist besser für den Schreiber, sich als Dummkopf ansehen zu lassen, als den Preis für die Aufdeckung seiner Pläne zu bezahlen". Und die *Argentis* empfahlen, absichtliche orthographische Fehler zu machen. Je höher gestellt jedoch die betreffende Person ist, um so weniger darf erwartet werden, daß sie die nötige menschliche Größe

---

[4] A propos Wortzwischenraum: Ihn zu unterdrücken, ist eine unumgängliche Vorsichtsmaßnahme der professionellen Kryptographie.

[5] Andrerseits wurde häufig /ch/ durch /q/ ersetzt. Bei der Kriegsmarine wurden manchmal Zahlen, deren Ziffern durch Buchstaben chiffriert waren, in /y/.../y/ eingeschlossen.

aufbringt, um sich mit verunstaltetem Text abzufinden. Der ideale Kryptosekretär (engl. *code clerk*, *cipher clerk*) muß also eine dichterische Sprache mit eiskalter Intelligenz und unter Verachtung jeder Orthographie beherrschen. Kein Wunder, daß man ihn selten findet. Und die Versuchung ist groß, 'radio' und 'station' getrennt zu codieren oder gar buchstabenweise, wie es ein fauler österreichischer Knabe tat und damit *Luigi Sacco* 1918 einen Einbruch ermöglichte (s. 13.4.1), oder Blender als Wortzwischenraum zu mißbrauchen, oder, wie eine französische Widerstandsgruppe, *tobacco* als Blender zu gebrauchen, was zwar ihren Nachschub erhöhte, aber auch zum Brechen einer doppelten Transposition führte. Dummheiten hatten oft verheerende Folgen. *"The sending of this one message must certainly have cost the lives of thousands of Germans"* schreibt *Moorman*, der Chef vom G.2A.6, im Hinblick auf den in 11.1.3 erwähnten Glücksfall vom 11. März 1918, durch den *Berthold* die Pläne für die deutsche Offensive vom 21. März 1918 bloßlegen konnte.

11.1.6 Zu den Führungsmerkmalen gehört daher Aufklärung darüber, wie kleinste Chiffrierfehler vom Feind ausgenützt werden können, und Überwachung. *Givierge* schreibt ≪*Chiffrez bien, ou ne chiffrez pas. En transmettant du clair, vous ne donnez qu'un renseignement à l'ennemi et vous savez lequel; en chiffrant mal, vous lui permettez de lire toute votre correspondance et celle de vos amis.*≫ Der gutgemeinte Rat darf allerdings nicht so großzügig ausgelegt werden, daß eine Chiffrierung von Funksprüchen ganz unterbleiben könnte. Dies geschah tatsächlich Ende August 1914 mit den Funksprüchen der russischen Narew-Armee *Rennenkampf*s in Ostpreußen, die unchiffriert in den Äther gingen, weil die Chiffrier- und Dechiffrierunterlagen noch nicht bei der Truppe eingegangen waren und weil es an Telephonverbindungen mangelte. Es ermöglichte *Hindenburg* und *Ludendorff* den Sieg in der Schlacht von Tannenberg samt Aufstieg zu Volkshelden. Umgekehrt: Die Deutschen verschlüsselten im 2. Weltkrieg Wettermeldungen und gaben damit, da das Wetter in Europa vorherrschend von West nach Ost zieht, oft zum Ansatz des ‚wahrscheinlichen Wortes' Anlaß; es wäre besser gewesen, solche unwichtigen Nachrichten im Klartext zu funken.

Rohrbach empfiehlt deshalb (s. 11.2.5), bei der Beurteilung der Sicherheit eines Verfahrens auch die Möglichkeit von Chiffrierfehlern einzubeziehen, da sie doch unausrottbar seien. Fragen der Abschirmung und Abwehr sind natürlich ebenfalls von großem Belang.

11.1.7 Die Verwendung memorierbarer Schlüssel (auch doppelter Schlüssel) gibt dem unbefugten Entzifferer eine Art Beweis in die Hand, wenn es ihm gelingt, den Schlüssel zu rekonstruieren, insbesondere wenn dieser etwas ‚bedeutet', das dem Absender ‚am Herzen liegt'.

11.1.8 Die Unbequemlichkeiten organisatorischer Art, die mit der Aufrechterhaltung der Chiffriersicherheit verbunden sind, sind nicht zu unterschätzen. Regelmäßiger Wechsel von Schlüsseln macht Arbeit. Trotzdem ist es schwer verständlich, daß das U.S. State Department noch 1917 so kurze Schlüssel wie

PEKIN und *POKES* verwendete, hatte doch schon *Porta* weise *CASTUM FODERAT LUCRETIA PECTUS ALGAZEL* als Schlüssel verwendet; die *Argentis* hatten schon Schlüssel wie *FUNDAMENTA EIUS IN MONTIBUS SANCTIS* und *GLORIOSA DICENTUR DE TE QUIA POTENTER AGIS* benutzt; *Vigenère* schrieb: „Je länger der Schlüssel ist, desto schwieriger ist die Chiffre zu brechen“.

Für polyalphabetische Chiffrierung ist es erforderlich, daß sie quasi-nicht-periodisch ist, d.h. daß der Schlüssel, wenn er periodisch ist, nicht wesentlich kürzer als die Nachricht ist. Notfalls muß eine Nachricht zerlegt und mit wechselndem Schlüssel chiffriert werden. *Hitts* Mahnung *“no message is safe in cipher unless the key phrase is comparable in length with the message itself”* bedeutet nicht, daß die Nachricht – auch bei Verwendung von Chiffriermaschinen – so lange wie die Periode des Schlüssels sein darf. Sprüche mit mehr als 1 000 Zeichen sind stark gefährdet, denn etwa bei der M-209 funktionieren die maschinellen Entzifferungstechniken (*pure cryptanalysis*, s. 22.2.3.1) gut ab einer Spruchlänge von etwa 800 Zeichen. Sprüche von 200-300 Zeichen sind normalerweise nicht gefährdet; bei der M-209 war die erlaubte maximale Länge 500 Zeichen, bei der ENIGMA waren es 180 Zeichen, nach Einführung der Rotoren VI - VIII (8.5.3) erhöht auf 250.

Der Gebrauch eines individuellen Einmal-Schlüssels bringt andrerseits zusätzliche organisatorische Belastungen und erfordert verstärkte Abschirmungs- und Abwehrmaßnahmen. Für manche Situation scheidet er damit von vornherein aus, so zum Beispiel für abgeschnittene Situationen, in denen kein oder kein sicherer Schlüsselnachschub gewährleistet ist, oder in Fällen, in denen der Feind einen in seine Hände gefallenen Vorrat an individuellen Schlüsseln zu einem ‚Funkspiel‘ weiterbenützen könnte.

11.1.9 Überhaupt ist es eine Frage, woran eine Funkstelle erkennt, ob der aufgefangene Spruch von ihrem Partner stammt oder von einem Dritten. Steganographische Maßnahmen (*‘Security Check’*), etwa darin bestehend, daß an bestimmten Stellen des Geheimtextes gewisse Blender eingefügt werden oder an bestimmten Stellen des Klartextes gewisse Buchstabierfehler gemacht werden (von der ‚Handschrift‘ der Funker ganz abgesehen) ergänzen die in 10.6 erwähnten kryptographischen Maßnahmen.

11.1.10 Zu guter Letzt ist die banalste und brutalste Art des kryptanalytischen Angriffs zu erwähnen: die Aneignung von Chiffrierunterlagen durch Ausspähung, Diebstahl, Raub oder Kampfmaßnahmen. Wie man sich dagegen schützt und wie wenig das oft nützt, liegt auf der Hand. Immerhin – was nicht mehr existiert, kann nicht in unbefugte Hände fallen. Dies beherzigte schon *Karl Weierstraß* im Hinblick auf die Briefe von *Sonja Kowalewskaya*. Es gilt in der kryptologischen Sicherheit ganz besonders für individuelle Schlüssel; am besten setzt man hinter das Chiffriergerät sogleich den Reißwolf (vgl. 8.8.2, Fußnote 12). Geradezu absurd ist deshalb die *geplante* Mehrfachverwendung eines individuellen Schlüssels (vgl. 8.8.7).

11.1.11 Es ist eine Binsenweisheit, daß Kampfhandlungen manchmal reiche Beute ergeben. Für kryptologisches Material trifft dies in besonderem Maße zu: Am 12. 2. 1940 wurde das deutsche Unterseeboot *U-33* im Firth of Clyde von der Royal Navy aufgebracht. Dabei vergaß der sonst sehr zuverlässige Maschinist *Kumpf*, drei ihm anvertraute Rotoren ins Meer zu werfen. Zwei von ihnen waren für die Briten neu, die Rotoren VI und VII (die Polen hatten die ersten fünf Rotoren aufgeklärt). Der Rotor VIII wurde im August 1940 ebenfalls erbeutet. Am 26. 4. 1940 wurde das deutsche Boot *Polares* vor Ålesund aufgebracht. Die Briten fanden zusammengehörige Klar- und Geheimtexte für die Tage vom 23. bis 26., die jedoch noch keinen vollen Einbruch in die ENIGMA-Chiffrierung der Kriegsmarine erlaubten. Auch die im Juni 1940 aus dem Unterseeboot *U-13* geholten Dienstvorschriften halfen noch nicht weiter. 1941 gelang jedoch der Durchbruch: Am 3. 3. 1941 wurden aus dem Boot *Krebs* im Vestfjord vor Norwegen nicht nur zwei schon bekannte Rotoren geholt, sondern auch die vollständigen Schlüsselunterlagen für den Monat Februar. Am 7. 5. 1941 führte ein geplanter Angriff auf das Wetterschiff *München* zu den vollständigen Schlüsselunterlagen für den Monat Juni (die für den Monat Mai und die ENIGMA selbst waren versenkt worden) und zum „Wetterkurzschlüssel“. Am 9. 5. 1941 wurde *U-110* westlich Irland durch Wasserbomben zum Auftauchen gezwungen und konnte von einer Mannschaft des britischen Zerstörers *HMS Bulldog* geentert werden; die Beute umfaßte neben einer (bereits nicht mehr unbekannten) ENIGMA einen kryptanalytischen Schatz von ENIGMA-Vorschriften, einschließlich der Bigrammtabelle BACH (4.1.2) für die Spruchschlüssel-Chiffrierung und das Kurzsignalheft, das reichlich für Kompromittierungen sorgte. Am 28. 6. 1941 schließlich fand nochmals ein geplanter Angriff auf ein Wetterschiff, die *Lauenburg*, statt; zwar gelang es den Deutschen, die ENIGMA zu versenken, aber die Briten erbeuteten die vollständigen Schlüsselunterlagen für den Monat Juli.

Damit hatte *Bletchley Park* den Durchbruch auch bei der 3-Rotor-ENIGMA der Kriegsmarine geschafft; der U-Boot-Funkverkehr konnte von da an regelmäßig, mit Verzögerungen von nur einigen Stunden, verfolgt werden. Dementsprechend verringerten sich die britischen Schiffsverluste.

Zwar kam ein Rückschlag mit der Einführung der 4-Rotor-ENIGMA am 1. 2. 1942, aber ab Dezember 1942 wurde der U-Boot-Funkverkehr wieder regelmäßig entziffert; die Allierten gewannen im U-Boot-Krieg die Oberhand. Ermöglicht wurde das wieder durch eine Kampfhandlung, die eine schier unglaubliche Dummheit des von *Eberhard Maertens* und *Ludwig Stummel* geleiteten Marinenachrichtendienstes ans Licht brachte: Die Aufbringung von *U-559* im Mittelmeer vor Port Said am 30. 10. 1942 durch den britischen Zerstörer *HMS Petard* ergab zunächst eine neue Ausgabe des Kurzsignalhefts und die zweite Auflage des Wetterkurzschlüssels und damit wieder reiche Kompromittierungsmöglichkeiten; dann fand am 13. 12. 1942 *Philip E. Archer* bei einer geglückten Entzifferung heraus, daß die 4-Rotor-ENIGMA im Verkehr mit Küstenstationen, die nur eine 3-Rotor-ENIGMA besaßen, den vierten Ro-

tor (die ‚Griechenwalze') einfach in Nullstellung gebrauchte – das erlaubte die Kommunikation. Die Dummheit bestand darin, daß die 3-Buchstaben-Grundstellung der 3-Rotor-ENIGMA grundsätzlich übereinstimmte mit den ersten drei Buchstaben der Grundstellung der 4-Rotor-ENIGMA. Das war reinste Bequemlichkeit in der Erarbeitung der Schlüsselunterlagen. War also die 3-Rotor-Grundstellung bereits ermittelt, waren nur 26 Versuche notwendig, um auch die Grundstellung der Griechenwalze zu finden. Die 4-Rotor-ENIGMA war nach dem 13. 12. 1942 im gesamten 1941 eingeführten ‚Triton'-Netz der U-Boote, von den Briten SHARK genannt, gebrochen; an der völligen Beherrschung des ENIGMA-chiffrierten Verkehrs bis Kriegsende änderte auch die Einführung einer zweiten Griechenwalze am 1. 7. 1943 nichts mehr.

Aber auch die Briten hatten Verluste hinzunehmen: Der deutsche Hilfskreuzer *Komet* erbeutete 1940 Codebücher und Bigramm-Chiffren der *Merchant Navy* (4.1.2, 4.4.3). Das erfuhren allerdings die Alliierten erst nach dem Krieg beim Studium deutscher Archive.

11.1.12 Es müssen nicht immer große Dinge sein, die dem Feind helfen: Auch kleinste Einzelheiten, die in seine Hände fallen, können verräterische Hinweise von großer Bedeutung geben.

Im August 1941 fiel das deutsche Unterseeboot *U-570* vor Island fast intakt in britische Hände. Der zur Aufbewahrung der ENIGMA dienende Holzkasten war leer, enthielt aber einen Hinweis auf einen vorsorglich vorgesehenen Platz für einen vierten Rotor. Dies (neben anderern Anzeichen in erbeuteten Manualen) warnte die Briten vor der bevorstehenden Einführung der 4-Rotor-ENIGMA (s. 11.2.1).

Aus einer Fülle von Kleinigkeiten erst setzt sich das Bild zusammen, vor dem erfolgreiche Kryptanalysis dauerhaft arbeiten kann, und jede Unterbrechung der Kontinuität des Mitlesens schädigt sie für lange Zeit oder für immer.

11.2 Maximen der Kryptologie

“The [ENIGMA] machine, as it was, would have been impregnable, if it had been used properly.”

Gordon Welchman 1982

“No cipher machine alone can do its job properly, if used carelessly. During World War II, carelessness abounded, particularly on the Axis side.”

Cipher A. Deavours, Louis Kruh 1985

“Hagelin [C38m] was virtually impregnable when used properly, as it was by Norway and Sweden.”

Ralph Erkine 1982

Über die Jahrhunderte hinweg hat sich in der Kryptologie ein reicher Schatz an Erfahrungen angesammelt – bereits die offene Literatur läßt dies erkennen. Aus diesen Erfahrungen entspringen Maximen für die kryptographische Arbeit, insbesondere für die Abwehr der unbefugten Entzifferung, die auch – oder gerade – in der heutigen Zeit der Materialschlachten nicht unberücksichtigt bleiben dürfen.

11.2.1 Zu den urtümlichsten Fähigkeiten des Menschen gehört, daß er sich in Sicherheit wiegen kann, daß er sich Mut machen kann und von der Gefahr sich nicht schrecken läßt. Daraus ergibt sich aber auch die

Regel Nr. 1: Man soll den Gegner nicht unterschätzen.

Bis zum Jahre 1944 schöpften, wie eingangs erwähnt, die deutschen Dienste keinen Verdacht, die Alliierten könnten die 3-Rotor-ENIGMA-Chiffrierung laufend mitlesen – lediglich die Marine ging am 1. 2. 1942 im U-Boot-Funkverkehr zur komplizierteren 4-Rotor-ENIGMA über[6] und führte auch drei zusätzliche Rotoren ein. Sie machte damit deutlich, daß es notwendig war, etwas für ihre Sicherheit zu tun. Der deutsche Generalstab war jedoch siegesgewiß; er war intellektuell nicht darauf vorbereitet, Warnungen ernstzunehmen. Aber selbst in der Kriegsmarine saß die Überzeugung von der Unüberwindbarkeit tief. Noch 1970 versicherte treuherzig Kapitän zur See *Heinz Bonatz*, ehemaliger Chef des B-Dienstes der Kriegsmarine, daß die Alliierten, obwohl ihnen ENIGMAs in die Hände gefallen seien, die deutsche Chiffrierung nicht gebrochen hätten; schlimmstenfalls hätten sie einige Sprüche entziffert. Nach den Enthüllungen von *Gustave Bertrand* 1973 und *Frederick Winterbotham* 1974 mußte er sein Buch umschreiben.

Nicht nur die deutsche Seite war arglos. Die Kryptanalytiker der Vereinigten Staaten konnten sich 1944 einfach nicht vorstellen, daß *Hans Rohrbach* ihre M-138-A Chiffrierung gebrochen hatte – allerdings nur ein kurzfristiger Erfolg, denn zu dieser Zeit führten die Amerikaner neue Chiffriermaschinen ein. Darunter war eine Rotormaschine ähnlich der ENIGMA, die M-134-C, auch SIGABA genannt. Die Signal Security Agency der U.S. Army hatte vergeblich versucht, zur Probe diese Chiffrierung zu brechen. Bedeutete das, den Deutschen würde es etwa nicht gelingen? Schließlich lasen die Engländer bereits seit Jahren die ENIGMA-Chiffrierung mit. Bezeichnenderweise mißtraute *Roosevelt*, der Intellektuelle unter den alliierten Staatsführern, den Beteuerungen der Kryptologen. Wußte er um die tiefverwurzelte menschliche Neigung, das Unerwünschte nicht zur Kenntnis nehmen zu wollen?

Die britische Marine bemerkte erst nach Jahren, daß der B-Dienst der deutschen Kriegsmarine einige ihrer Chiffrierungen mitlas. ENIGMA-Entzifferun-

---

[6] Schon 1930 hatte der Leutnant *Henno Lucan*, zweiter Nachrichtenoffizier des Schlachtschiffes Elsaß, in einer Studie darauf hingewiesen, daß die ENIGMA kryptologisch nicht sicher sei. Mit der Einführung des Steckerbrettes schienen jedoch die Bedenken geringer geworden zu sein.

gen gaben schließlich den unumstößlichen Hinweis, daß zumindest *Naval Cypher No.* 3, das hauptsächliche Chiffrierverfahren für die Konvois im Nordatlantik (deutscher Deckname ‚Frankfurt‘) bloßgestellt war. Es wurde durch *Naval Cypher No.* 5 ersetzt, und damit waren die Deutschen, wie sich nach dem Krieg herausstellte, von Mitte 1943 an von der Quelle ziemlich abgeschnitten. Was wäre wohl geschehen, wenn die Deutschen auf ähnliche Weise die Unzuverlässigkeit ihrer ENIGMA herausgefunden hätten?

Vielleicht nichts, wie ein besonders krasser Fall der ständigen Unterschätzung der Briten durch Konteradmiral *Eberhard Maertens* und seinen Stabschef *Ludwig Stummel* zeigt. Er passierte Mitte 1943: Von den Deutschen entzifferte Funksprüche zeigten, daß die Amerikaner zwanzig U-Boote in einem engen Planquadrat vermuteten. Tatsächlich befand sich dort das Rudel mit dem Decknamen ‚Meise‘. Der Befehlshaber der Untersee-Boote, Großadmiral *Dönitz* (1891–1980), befahl *Maertens* “..... *to investigate, as he had done in 1941.*[7] *Again Maertens exculpated ENIGMA. The British U-boat situation reports themselves stated that the Allies' information on submarine locations was coming from direction-finding, he said*” (nach *Kahn*). *Maertens* rettete sich also mit einer falschen Erklärung durch das am 2. 2. 1943 in einem abgeschossenen britischen Bomber gefundene, mit Zentimeter-Wellen arbeitende Radar-Gerät („Rotterdam-Gerät“). *Dönitz* mußte sich zufrieden geben. Er war aber nie völlig beruhigt, insbesondere als am 12. März 1944 wieder ein Vorfall nur mit mangelhafter Chiffriersicherheit oder Verrat erklärt werden konnte. Wenigstens fand er bald eine Gelegenheit, *Maertens* auf ein Heimatkommando zu versetzen. Sein Nachfolger, der zum Konteradmiral beförderte *Stummel*, sang das selbe Lied. Insgeheim aber war er gewillt, die Sicherheit des U-Boot-Funkverkehrs zu verbessern, und führte für jedes Boot seinen eigenen Schlüssel ein – eine halbherzige und, wie sich zeigen sollte (s. 19.4.1), sogar gefährliche Maßnahme.

Den Russen gelang ebenfalls gelegentlich ein Einbruch in die ENIGMA-Chiffrierung. So wurde von ihnen das am 30. Juli 1944 versenkte *U-250* gehoben und daraus eine ENIGMA geborgen. Es gibt geteilte Meinungen darüber, wie weit die Russen erfolgreich waren. In einer Besprechung der Funksachbearbeiter im OKL wurde im Januar 1943 festgestellt: „Es steht mit Sicherheit fest, daß den Russen in Einzelfällen die Entzifferung von ENIGMA-Sprüchen gelungen ist.“ *E. E. Thomas* andrerseits sagte 1978, daß er in zehnjährigen detaillierten Studien keinen Anhaltspunkt fand, daß die Russen jemals deutsche Funksprüche mitgelesen hatten.

Ob die Russen in die Chiffrierverfahren der U.S.A. eindrangen, wurde oft diskutiert, insbesondere nachdem *Isaac Don Levine*, ein Journalist russischer Herkunft, der sich auf russische Angelegenheiten spezialisiert hatte, erklärt

---

[7] *Dönitz* schrieb 1959 in seinen Memoiren, daß der Verdacht, der Feind könnte mitlesen, Ende 1941 durch eine gründliche Untersuchung ausgeräumt worden sei. Da war wohl bei einigen seiner Leute, wie Admiral *Maertens* und Kapitän *Stummel*, der Wunsch der Vater des Gedankens.

hatte, er sei "convinced by mid-1939 from numerous conversations he had with General *Walter Krivitsky*, the defected head of Soviet military intelligence for Western Europe, that the Communist cryptanalysts were reading American codes" (*Kahn*).

11.2.2 Harmlos, aber besonders gefährdet sind in dieser Hinsicht die Erfinder von Chiffrierverfahren. *"Nearly ervery inventor of a cypher system has been convinced of the unsolvability of his brainchild"*, schreibt *Kahn*. Ein tragikomisches Beispiel bietet *Bazeries* selbst. Als Beauftragter der französischen Regierung und Armee hatte er zahlreiche ihm vorgelegte Erfindungen ruiniert, indem er probeweise die Chiffrierung brach. Ausgerechnet ihm fiel dann selbst ein System ein, das er prompt als absolut sicher bezeichnete. Der *Marquis de Viaris*, dessen Erfindung *Bazeries* kurz zuvor abgeschmettert hatte, rächte sich: Er gab (vgl. 7.5.3) sogar eine Methode an, um bei Kenntnis der Alphabete *Bazeries* Chiffrierung und damit die ganze Klasse von *Jefferson* bis M-138-A zu brechen (s. 14.3). Hier kommen wir auf die

Regel Nr. 2: Nur der Kryptanalytiker, wenn überhaupt jemand, kann die Sicherheit eines Chiffrierverfahrens beurteilen.

Diese Erkenntnis, die man bis *Porta* und *Rossignol*[8] zurückverfolgen kann, formulierte *Kerckhoffs*[9] 1883. Er kritisierte, die kryptanalytische Sicherheit eines Verfahrens dadurch demonstrieren zu wollen, daß man abzählt, wieviele Jahrhunderte es dauerte, um alle möglichen Kombinationen zu durchlaufen: ≪*Je suis stupéfait de voir nos savants et nos professeurs enseigner et recommander pour les usages de la guerre des systèmes dont un déchiffreur tant soit peu expérimenté trouverait certainement la clef en moins d'une heure de temps.*≫

In der Tat können solche Abzählungen nur eine obere Schranke geben, sie betreffen die Zeit, die die ineffizienteste aller kryptanalytischen Methoden, die *exhaustive Suche* (engl. auch '*brute force attack*') braucht.

Auf der ganzen Welt haben deshalb die staatlichen Dienste (und einige nichtstaatliche) die doppelte Aufgabe, sichere Chiffrierverfahren zu entwerfen und angeblich sichere Chiffrierverfahren zu brechen. "*With code breakers and code makers all in the same agency, N.S.A. has more expertise in cryptography than any other entity in the country, public or private*" schrieb nicht ganz ohne Stolz *Stewart A. Baker*, ein berühmter Anwalt, der zeitweilig für die *National Security Agency* tätig war. Er hätte besser geschwiegen.

11.2.3 *Kerckhoffs* war einer der ersten, der die Kryptographie von einem praktischen Standpunkt aus diskutierte. So schreibt er: ≪*il faut bien distinguer entre un système d'écriture chiffrée imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondence des differents*

---

[8] *Antoine Rossignol*, im Dienste *Ludwig* XIV. Erfinder der zweiteiligen Codebücher.

[9] *Auguste Kerckhoffs* (1835–1903), flämischer Professor. Verfasser von ≪*La cryptographie militaire*≫, 1883.

chefs d'armée entre eux≫ und erörterte Fragen der Handhabbarkeit, auf die wir noch zurückkommen werden. Er unterschied erstmals klar zwischen dem eigentlichen Schlüssel und der Verfahrensklasse (*système*) und postulierte ≪*Il faut qu'il puisse sans inconvénient tomber entre les mains de l'ennemi*≫.

Regel Nr. 3: Bei der Beurteilung der kryptanalytischen Sicherheit eines Verfahrens muß man damit rechnen, daß dem Gegner die Verfahrensklasse bekannt ist: „Der Feind kennt das benutzte System" (*"The enemy knows the system being used"*, *Shannon 1949*).

Aus praktischen Gründen kommen in gewissen Situationen gewisse Verfahren vorzugsweise, andere gar nicht zur Verwendung. Insbesondere das zähe Beharren des etablierten Apparats läßt gewisse Vorlieben entstehen, die dem Gegner nicht verborgen bleiben (‚Chiffrierphilosophie'). Auch lassen schon die einfachsten kryptanalytischen Tests zuverlässig eine Unterscheidung zwischen monoalphabetischer Substitution, polyalphabetischer Substitution und Transposition zu;[10] sogar die Periode einer polyalphabetischen Substitution oder die Breite einer Transposition läßt sich dank *Kasiski*, *Kerckhoffs* und *Friedman* finden.

Geräte können im übrigen bei Kampfhandlungen in gegnerische Hände fallen oder gestohlen werden. Dies schließt Chiffriermaschinen wie die ENIGMA ein; hätte man *Kerckhoffs'* Lehre befolgt, hätte die ENIGMA bereits zu Beginn des 2. Weltkriegs mindestens zur 5-Rotor-Maschine erweitert werden müssen, und die einzelnen Rotoren hätten nicht erst ab 1942 dreimal täglich gewechselt werden müssen; vor allem hätte alle paar Monate der ganze Rotorsatz ausgewechselt werden müssen. Natürlich wäre das kein leichtes gewesen; schätzt man doch (vgl. 7.3.3), daß an die 100 000 ENIGMAs insgesamt gebaut und verwendet wurden. Aber auch die Amerikaner waren in diesem Punkt verletzbar. Ihre auf mittlerer Gefechtsebene verwendete Chiffriermaschine M-209, nach der Konstruktion von *Hagelin* in Lizenz gebaut, war bedeutend weniger sicher als die ENIGMA und wurde auch von der italienischen Marine (C-38m) benutzt. Kein Wunder, daß die Deutschen von 1942 bis 1944 in Nordafrika und Italien über Angriffszeiten und -ziele der amerikanischen Truppen oft genug Bescheid wußten, aber auch die Briten über den Nachschub des Feldmarschalls *Rommel*.

11.2.4 Das Bestreben des Kryptologen, es dem Gegner nicht zu leicht zu machen, führt ihn dazu, Komplikationen von bekannten Verfahren zu ersinnen. Seit alters her dient dazu die Komposition von Verfahren (9. Kapitel). Zweimalige Substitution ist wieder eine Substitution, zweimalige Transposition eine Transposition, bringt also nichts. Mehr kann man sich von der Kombination *verschiedener* Verfahren versprechen. Codierung mittels Codebüchern wird polyalphabetisch ‚überchiffriert' (9.2), monoalphabetische Substitution

[10] Ein von *Sacco* aufgestelltes Kriterium lautet: Ein kurzer Geheimtext von nicht mehr als, sagen wir, 200 Zeichen, in dem alle Alphabetzeichen vorkommen, ist höchstwahrscheinlich polyalphabetisch chiffriert.

wird zusätzlich einer Transposition unterworfen, etc. Spezifische kryptanalytische Methoden sind jedoch oft gegen solche Komplikationen unempfindlich. Es gilt (*Givierge* 1924)[11]

Regel Nr. 4: Äußerliche Komplikationen können illusorisch sein; sie gaukeln dann dem Kryptologen eine trügerische Sicherheit vor.

Im schlimmsten Fall kann eine illusorische Komplikation sogar die unbefugte Entzifferung erleichtern. Wird etwa bei einem VIGENÈRE-Verfahren in bester Absicht die identische Substitution ausgeschlossen, so geht niemals ein Buchstabe in sich über. Damit kann aber die Lage eines hinreichend langen ‚wahrscheinlichen Wortes' im Text ziemlich sicher festgestellt werden. Die selbe Eigenschaft haben alle echt involutorischen Alphabete. Bei der ENIGMA wurde durch eine Reflexion an der letzten Scheibe die Zahl der Rotoren, durch die die Signale gingen, verdoppelt; es entstand aber dadurch eine echt involutorische Chiffrierung, die den Polen und Briten den in 11.2.1 erwähnten Einbruch ermöglichten, s. 14.1, 19.6.2. Auch die Zylinder- und Streifen-Geräte (7.4.3) von *Jefferson* und *Bazeries*, die M-94 und die M-138-A, haben die verräterische Eigenschaft *"no letter may represent itself"*. Dazu bemerkte *Welchman "It would also have been possible, though more difficult, to have designed an Enigma-like machine with the self-encipherment feature, which would have knocked out much of our methodology, including females"*.

11.2.5 Schließlich als letzter und vielleicht wichtigster Punkt ist die menschliche Schwäche zu vermerken. Eine Chiffrierung ist nicht besser als der **Kryptosekretär**. Die unbefugte Entzifferung lebt von den **Chiffrierfehlern**, wie sie schon in 11.1 besprochen wurden.

Zuallererst müssen die Kompromittierungen des Schlüssels genannt werden:

Klartext-Geheimtext-Kompromittierung: die Wiederholung der Übertragung im Klartext,

Geheimtext-Geheimtext-Kompromittierung: die Übertragung zweier *isologs*, d.h. des selben Klartextes, mit zwei verschiedenen Schlüsseln chiffriert,[12]

Klartext-Klartext-Kompromittierung: die Übertragung zweier verschiedener Klartexte, mit dem selben Schlüssel chiffriert.

Sodann kommen die Fehler, die Futter für einen Angriff (engl. *cribs*) liefern:

der häufige Gebrauch stereotyper Wörter und Wendungen (wofür die Sprachen der Diplomaten und Militärs so reichlich Anlaß geben),

der Gebrauch zu kurzer und leicht erratbarer Schlüsselwörter,

der Gebrauch eines geläufigen Wortes für ein plötzlich eingetretenes Ereignis (‚wahrscheinliches Wort').

---

[11] *Marcel Givierge*, französischer General, erfolgreicher Kryptologe im 1. Weltkrieg. Verfasser von ≪*Cours de Cryptographie*≫, Paris 1925.

[12] Insbesondere die in Kapitel 10 besprochenen Öffentlichen Schlüssel laden dazu ein.

Schließlich sind die Verstöße gegen elementare Regeln einer guten kryptographischen Sprache zu nennen:

der Nichtgebrauch von Homophonen und Blendern bei Benutzung von Codebüchern,
der Gebrauch von Buchstabenverdoppelungen und -kombinationen wie *ch* und *qu*, Interpunktionszeichen und vor allem
der Gebrauch des Wortzwischenraumes.

Der ideal zur Chiffrierung vorbereitete Klartext ist orthographisch falsch, sprachlich knapp, stilistisch grauenhaft. Welcher Kommandierende General will einen Befehl so abfassen, welcher Botschafter einen Bericht an sein Staatsoberhaupt, welcher Geschäftsmann will so einen Brief absenden? Die Antwort lautet: Die *cipher clerks* müssen die schmutzige Arbeit tun. Sogar *Churchill* unterwarf sich den Unbequemlichkeiten der Chiffriersicherheit.

Erschwerend kommt aber hinzu, daß Botschafter, Generäle und Generaldirektoren eigentlich ihre *cipher clerks* überwachen sollten, sich aber selten die Zeit nehmen. In der Regel fehlt ihnen auch das Verständnis für die Notwendigkeit; meist sind sie kryptologisch ignorant. Als *Wheatstone* ein spezielles Bigramm-Substitutions-Verfahren erfand, das später PLAYFAIR genannt wurde (4.2), konnte er die Abneigung des Foreign Office gegen komplizierte Chiffrierung nicht überwinden (vgl. 2.1.1). *Napoleon*s Generäle chiffrierten ihre Nachrichten nur teilweise, und so taten es auch noch 1916 die Italiener.

Ein altbewährter Grundsatz des Nachrichtenwesens ist deshalb: Die Überwachung eigener und verbündeter Einheiten ist mindestens so wichtig wie die Beobachtung der gegnerischen. Dazu schrieb *Hüttenhain*: „Ein Verbündeter, der keine sicheren Chiffrierungen verwendet, stellt ein potentielles Risiko dar.

“A cryptographer’s error is the cryptanalyst’s only hope”, sagt man, und diese Hoffnung ist berechtigt. Zu bedenken ist natürlich die nervliche Belastung, unter der ein Chiffrierer im militärischen und diplomatischen Verkehr steht. Ein Chiffrierfehler passiert da leicht. Je komplizierter das Verfahren, umso mehr verstümmelten Klartext erhält der Dechiffrierer. Die gefährliche Wiederholung der gleichen Nachricht (ohne gründliche Umformulierung) mag dann unter Zeitdruck unvermeidlich sein. Dementsprechend schrieb *Givierge* (vgl. 11.1.6) *≪Chiffrez bien, ou ne chiffrez pas≫*. *Rohrbach* formulierte die

Regel Nr. 5: Bei der Beurteilung der kryptanalytischen Sicherheit eines Verfahrens sind Chiffrierfehler und andere Verstöße gegen die Chiffrierdisziplin mit einzubeziehen.

Der gute Kryptologe weiß, daß er sich auf nichts verlassen kann, nicht einmal darauf, daß der Feind bei seinen Fehlern bleibt, und ist besonders kritisch gegenüber seinen eigenen möglichen Fehlern. Die Überwachung der eigenen Chiffriergewohnheiten durch einen *advocatus diaboli* ist, wie die Erfahrungen der Deutschen im 2. Weltkrieg zeigten, unbedingt notwendig. *Stuart Milner-Barry* schrieb *“Had it not been for human error, compounded by a single design quirk, the Enigma was intrinsically a perfectly secure machine”*.

Der *design quirk*, die anscheinend schlaue Idee (7.3.2) war der durch die Einführung der Umkehrscheibe bewirkte echt involutorische Charakter der Chiffrierung; eine betriebliche Erleichterung wurde mit einer gefährlichen Einbruchsmöglichkeit erkauft.

11.3 Shannons Maßstäbe

Claude E. Shannon hat fünf Maßstäbe zusammengestellt, die an eine kryptographische Verfahrensklasse angelegt werden sollten:[13]

(1) *Kryptanalytische Sicherheit*	Wieviel besser ist derFeind dran, wenn er eine gewisse Menge Material empfangen hat?
(2) *Schlüssellänge*	Wie kurz ist der Schlüssel, wie einfach ist er handzuhaben?
(3) *Praktische Durchführung der Chiffrierung und Dechiffrierung*	Wieviel Arbeitsaufwand ist notwendig?
(4) *Aufblähung des Geheimtextes*	Um wieviel länger ist der Geheimtext als der Klartext?
(5) *Verschleppung von Chiffrierfehlern*	Wie weit kann eine Verschleppung von Chiffrierfehlern stattfinden?

Diese Beurteilungsmaßstäbe sind insofern widersprüchlich, als kein System bekannt ist (und wohl auch logisch ausgeschlossen ist), das in allen Punkten maximale Anforderungen erfüllt. Andererseits kann man in keinem der Punkte ganz anspruchslos sein. Läßt man 1) völlig fallen, so ist selbst Klartext zulässig. Läßt man 2) völlig fallen, so kann ein individueller Einmal-Schlüssel alle anderen Punkte optimal erfüllen. Läßt man 3) und 4) fallen, so kann man unschwer exotische Systeme finden, die allen anderen Ansprüchen gerecht werden. Läßt man 5) fallen, so ist mit Verfahren, die gründlich genug durchmischen (vgl. 9.4.3), alles andere beliebig gut erreichbar.

Die moderne Kryptographie neigt, je nach der Situation, den individuellen Schlüsseln (die ungehinderten Schlüsselnachschub erfordern) oder den Durchmischungsverfahren (die absolut störfreie oder hochgradig störgesicherte Nachrichtenverbindungen erfordern) zu.

Kommunikation von äußerster Geheimhaltungsnotwendigkeit, sagen wir Angelegenheiten zwischen Staatsmännern in Notsituationen, kann sehr wohl durch individuelle Einmal-Schlüssel abgewickelt werden, da dies normalerweise nicht viele Nachrichten erfordert. Aber selbst bei heftigem Nachrichtenverkehr kann dies angezeigt sein. *Frederick W. Winterbotham*, für die

[13] *C. E. Shannon*, A Mathematical Theory of Cryptography. Interner Bericht, 1. September 1945. Publiziert als: Communication Theory of Secrecy Systems. Bell System Technical Journal **28**, 656-715 (October 1949).

Sicherheit der unter dem Decknamen ULTRA erzielten britischen Auswertungen des ENIGMA- und des SZ42-Funkverkehrs verantwortlich, bestand darauf, daß durch Funk übermitteltes ULTRA-Material mit einem individuellen Schlüssel chiffriert wurde, trotz der damit verbundenen Umständlichkeit. Dies zeigt, wie kostbar das Material war, und wie hoch die Briten dieses Kryptosystem, sicher zu recht, einschätzten. Hätte er sich einem deutschen General gegenüber damit durchsetzen können?

Im kommerziellen Bereich wird mit dem DES-Verfahren seit Jahren ein typisches Durchmischungsverfahren bevorzugt. Der anhaltenden Kritik an der kryptanalytischen Sicherheit des derzeitigen *de facto* Standards wäre mit einer Vergrößerung der als zu klein angesehenen Schlüssellänge (9.6.5) einiger Wind aus den Segeln genommen.

11.4 Kryptologie und Grundrechte

Seit kryptographische Methoden angewendet werden, wird versucht, sie zu brechen. Für Amateure, auch wenn sie sich mittelgroßer Maschinen bedienen, dürften die Schwierigkeiten allerdings enorm sein, in eine Chiffrierung, die professionellem Standard genügt, einzudringen. Die *National Security Agency* (N.S.A.) der U.S.A. aber wird vermutlich in der Lage sein, eine unter Verdacht geratene kommerzielle Verbindung zu überwachen. Schließlich darf man annehmen, daß die Regierung der Vereinigten Staaten von Amerika nicht unter dem Deckmantel eines kommerziellen Nachrichtennetzes einem gegnerischen Nachrichtendienst – noch gibt es solche – ungehinderte Arbeitsmöglichkeiten eröffnen will. Die Zeiten sind vorüber, zu denen *Henry L. Stimson*, Unterstaatssekretär von Präsident *Hoover*, den Dechiffrierdienst des State Departments in die Wüste schicken konnte (1929!) und dazu in seiner Autobiographie die Begründung nachschieben konnte *“Gentlemen do not read each other's mail”*. Nicht einmal Präsident *Carter* zeigte ähnliche moralische Skrupel. Oder ist das vielleicht ein Anzeichen dafür, daß es den Amerikanern nicht gelungen ist, bei den Russen mitzulesen? Das Ende des Kalten Kriegs bedeutet nur eine Abschwächung, aber keine Beendigung der latenten Gefahr, ausgespäht zu werden.

11.4.1 Die Kryptologie ist aber nicht nur eine Angelegenheit der diplomatischen und militärischen hoheitlichen Dienste. Man soll sich nicht darüber hinwegtäuschen, daß auch der prinzipiell bestehende Interessenkonflikt zwischen dem einzelnen Staatsbürger und dem Staat als Vertreter des gesamten Staatsvolks durch die Kryptologie berührt wird: Auf der einen Seite steht der unabweisbare Wunsch des einen oder anderen Staatsbürgers (oder einer juristischen Person), seine Privatsphäre (oder ihre kommerziellen Interessen) durch wirksame Chiffriersysteme zu schützen, auf der anderen Seite steht die Wahrung der inneren und äußeren Sicherheit des Staates, der zwecks Erlangung nachrichtendienstlicher Erkenntnisse auch in chiffrierte Nachrichten eindringen will.

Den Standpunkt der einen Seite faßte *Charles A. Hawkins*, Acting Assistant Sectretary of Defense, U.S.A. so: "*The law enforcement and national security communications argue that if the public's right to privacy prevails and free use of cryptography is allowed, criminals and spies will avoid wire taps and other intercepts*". Schon das Brief-, Post- und Fernmeldegeheimnis ist eben nicht absolut und kann unter Umständen, die im einzelnen zu regeln sind (in Deutschland sehr restriktiv im Gesetz zu Artikel 10 des Grundgesetzes vom 13. Aug. 1968) durchbrochen werden – allerdings nicht von Privatpersonen, denen dies bei Strafe (in Deutschland §202, §354 StGB) verboten ist. Chiffrierte Nachrichten werden dabei besonderes Interesse finden – schon der Gebrauch kryptologischer Mittel bringt eine Nachricht unter Verdacht.

Andrerseits wird gerade in den Vereinigten Staaten von Amerika, wo jeder Bürger den Besitz einer Feuerwaffe als unverzichtbares Privileg ansieht, auch der Besitz der Waffe CRYPTO nicht gerne dem staatlichen Monopol überlassen. Europa, mit seiner etwas gelasseneren Tradition, ist zurückhaltender.

Diffie brachte es auf die kurze Formel: "*...an individual's privacy as opposed to Government secrecy*". In Europa haben wir allen Grund, auf der ‚Freiheit vom Obrigkeitsstaat' zu bestehen. Es muß also im Rahmen der jeweiligen Staatsverfassung eine Regelung für die staatliche Kryptanalysis gefunden, eine Grenzlinie gezogen werden. Dies verlangt schon die Rechtssicherheit. Seltsamerweise hängt hier schon bei den Großmächten die Entwicklung der Gesetzgebung stark zurück. Es ist insbesondere an den internationalen Handel zu denken. Aus der Sicht der U.S.A. gilt für den Verkehr mit kryptologischem Gerät: "*Encryption for the purpose of message authentication is widely allowed, whereas encryption for the purpose of keeping information private raises eyebrows*" (*David S. Bernstein*). Somit mußte, nach Einschätzung seines Rechtsanwalts, der U.S.Amerikaner *Philip R. Zimmermann* eine Anklage wegen Verletzung der Bestimmungen der *International Traffic in Arms Regulations* befürchten, weil er 1991 zur freien Verfügbarkeit in das *Internet* das kryptographische System PGP (*Pretty Good Privacy*) entweichen ließ (9.6.6), das unter die Kriegsmaterial-Liste fällt ("*cryptographic devices, as well as classified and unclassified data related to cryptographic devices*", Category XIII). Die 1993 aufgenommenen Ermittlungen wurden 1996 fallengelassen; aber daß es überhaupt zu solchen kommen konnte, ist unbefriedigend.

11.4.2 Für eine Regelung des Konflikts, die einerseits den Schutz der Privatsphäre des gesetzestreuen Bürgers und die Vertraulichkeit von Nachrichten, andrerseits die Erfüllung von Aufgaben der Staatsmacht gewährleistet, zeichnen sich bereits verschiedene Ansätze ab:

1) Die Begrenzung der Verwendung von Chiffriersystemen im zivilen Bereich durch Genehmigungspflicht im Einzelfall und/oder nach Typenmustern kommerzieller Vertreiber (das Verbot gewisser Verfahren allein, soweit es nicht der Gebrauch individueller Schlüssel ist, reicht nicht aus, da es zu Umgehungen reizt).

(2a) Die Einschränkung der kryptanalytischen Sicherheit mittels Verfügbarmachung geeigneter Chiffriersysteme im zivilen Bereich. Die für die Verfügbarmachung eingerichtete Behörde kann gleichzeitig eine dem Staatsbürger dienliche kryptanalytische Sicherheitsprüfung vornehmen und so den Anreiz zur freiwilligen Unterwerfung erhöhen (ein kommerzieller Vertreiber kann als ‚Marktführer mit Staatshilfe') dienen.

(2b) Wie (2a), aber gekoppelt mit dem Verbot des Gebrauchs anderer Chiffriersysteme im zivilen Bereich.

(3) Die Hinterlegungspflicht der vollständigen Kenndaten jedes einzelnen im zivilen Bereich verwendeten Chiffriersystems bei einer zur Verschwiegenheit verpflichteten Behörde.

Weitere Regelungen sind denkbar, sowie Übergänge zwischen den oben aufgezählten. Man muß damit rechnen, daß verschiedene demokratische Staaten im Rahmen ihrer Souveränität zu verschiedenen Lösungen greifen werden. So war in Frankreich lange Zeit eine rigorose Regelung nach (1) in Kraft, die man aber als undemokratisch bezeichnen könnte, und die Niederlande liebäugelten mit einer solchen. Im Januar 1999 hob die französische Regierung die Genehmigungspflicht, die ohnehin unterlaufen wurde, auf.

In Deutschland besteht seit längerem eine Tendenz zur Regelung nach (2) (Bundesamt für Sicherheit in der Informationstechnik, BSI) – die liberale Grundhaltung wurde im Juni 1999 vom Bundeskabinett bestätigt.

Welche Regelung die Regierung Großbritanniens sucht, ist immer noch nicht abzusehen. In den U.S.A. wurde schon 1993 eine Regelung nach (3) von der Clinton-Administration ins Gespräch gebracht ('*key escrow system*', s.u.). Auf lautstarke Proteste hin wurde eine Art Freiwilligkeit der Unterwerfung in Aussicht gestellt, die etwas in die Richtung von (2a) geht. Noch im Jahr 1999 war in den U.S.A. der Kampf nicht entschieden.

Für die Europäische Union, sofern sie in dieser Frage überhaupt zu Ergebnissen kommt, scheiden wohl (1) wie (3) aus. Anfang Dezember 1998 erfolgte im Rahmen des Wassenaar-Abkommens (s. 11.4.6) eine gewisse Richtlinie der Exportkontrolle auf einer mittleren, liberalen Linie. Insbesondere sollen Geräte mit 64-Bit-Spruchschlüsseln frei bleiben.

Im übrigen kann man sich vorstellen, welches Durcheinander solcherart verschiedene Regelungen insbesondere für supranationale kommerzielle Anbieter schaffen würden. Der grenzüberschreitende Verkehr ist schon schwierig genug: "*International use of encryption plunges the user headfirst into legal morass of import, export and privacy regulations that are often obscure and sometimes contradictory" (David S. Bernstein).* Wer mit seinem *laptop computer* auf Reisen ging, machte sich möglicherweise strafbar. *Martha Harris*, Deputy Assistant Secretary of State for Political-Military Affairs, stellte am 4. Februar 1994 fest: "*We will no longer require that U.S. citizens obtain an export license prior to taking encryption products out of the U.S. temporarily for their own personal use. In the past, this requirement caused delays and inconvenience for business travellers.*" Liberalität ist auf dem Vormarsch.

11.4.3 Der 1994 verabschiedete *Escrowed Encryption Standard*[14] umfaßt den Chiffrieralgorithmus SKIPJACK (9.6.5) innerhalb des CLIPPER-Chip. Hinterlegt werden zwei *chip unique key components*, die erst auf richterliche Anordnung durch eine binäre Addition den *chip unique key* ergeben. Ein zwischen zwei Partnern zu verabredender, für Chiffrieren und Dechiffrieren benutzter 80-Bit-Spruchschlüssel (*session key*) KS dient wie c_0 bei DES als Initialisierungsblock, er wird je nach dem Betriebsmodus monoalphabetisch oder zur Verkettung benutzt. In einem *Law Enforcement Access Field* (LEAF) wird in individuell codierter Form dieser Spruchschlüssel abgespeichert; durch den *chip unique key* erhält man den echten Spruchschlüssel zurück. Eine Abhör- oder Abschreibvorrichtung, die den *chip unique key* bekommen hat, kann demnach jede mit einem neuen Spruchschlüssel startende Verbindung laufend mithören oder -schreiben, da auch LEAF (zusammen mit einem 32-Bit-Chipidentifikator und einer 16-Bit-Quersumme) übertragen wird, sofern diese Übertragung korrekt ist.

Der SKIPJACK-Algorithmus selbst – er fand übrigens außerhalb des staatlichen Bereichs, für den er vorgeschrieben war, wenig Verwendung – wurde (anders als DES) von der Behörde zunächst geheimgehalten, weil „andernfalls die Funktion des LEAF unterlaufen werden könnte“ – die Chiffriersicherheit selbst erforderte diese Geheimhaltung nicht. Der Algorithmus war ferner eingestuft als SECRET – NOT RELEASABLE TO FOREIGN NATIONALS und auch damit als internationaler *de facto* Standard ungeeignet. 1998 wurden diese Beschränkungen endlich aufgehoben.

Bei Licht betrachtet, ist die Technik des *Law Enforcement Access Field* ziemlich primitiv. Es liegt auf der Übertragungsstrecke offen; auch nichtautorisierte Entzifferer könnten sich daran versuchen. *Dorothy E. Denning* hat einige der praktischen Fragen, die sich ergeben, untersucht; *Silvio Micali* (‘Fair Cryptosystems’, U.S. Patent 5 276 737 vom 4. Januar 1994) hat weitreichende Lösungsvorschläge gemacht für ein kryptographisches System, das weder von Kriminellen noch von der Staatsmacht mißbraucht werden kann. Für interaktive Realzeitsysteme haben *Thomas Beth* und andere 1994 vorgeschlagen, die Staatsschutzbehörde zu einem aktiven Teilnehmer in dem Schlüsselvereinbarungs-Protokoll zwischen zwei Partnern zu machen, ohne daß ihre Einschaltung von den Partnern bemerkt werden kann. Die Neuheit dieses Ansatzes liegt darin, daß im Falle einer Nichteinschaltung der überwachenden Stelle der Netzwerkbetreiber dies beweisen kann und damit ein Mißbrauch durch eine *totalitäre* Staatsmacht auszuschließen ist.

11.4.4 Das Mißtrauen des einen oder anderen Staatsbürgers und der juristischen Personen gegenüber der Staatsgewalt wird nicht gerade abgebaut durch die Erfahrungen, die er mit dieser macht, etwa in den U.S.A. mit tatsächlichen oder unterstellten Eingriffen der *National Security Agency* in

[14] *Escrowed Encryption Standard* (EES), Federal Information Processing Standards Publication (FIPS PUB) 185, Feb. 9, 1994.

die Entwicklung von Chiffrieralgorithmen, beginnend mit DES. Der N.S.A. die Verantwortung für die Genehmigung und Empfehlung von Chiffrieralgorithmen zu geben, wird mancherorts als Farce empfunden (*"like putting the fox in charge of guarding the hen house"*, *Philip Zimmerman*, PGP User's Guide, 1994).

Bereits 1957 gab es Gerüchte über enge Kontakte und den Verdacht von Absprachen zwischen *William F. Friedman* und *Boris Hagelin*, die sich ja aus Kriegszeiten kannten (8.5.2).



Boris Hagelin
(1892–1983)

Damit ist der Dritte im Bunde genannt, der zwar außerhalb der Staatsrechtsphilosophie einer Balance zwischen den verfassungsmäßigen Rechten des Bürgers und der Staatsgewalt steht, aber angesichts seiner wirtschaftlichen Bedeutung nicht übergangen werden kann: der kommerzielle Anbieter. Sein Interesse ist es, sich mit dem Staatsbürger (und dem Unternehmer) als potentiellem Kunden ebenso gut zu stellen wie mit dem Staat als Überwachungsorgan. Günstigstenfalls ist der kommerzielle Anbieter ein ehrlicher Makler.

Erschwert wird diese Rolle allerdings durch eine gewisse Unehrlichkeit, die die Staatsbehörden dem kommerziellen Anbieter aufzwingen, indem sie ihm bei Auslandsgeschäften Auflagen machen, die bei Inlandsgeschäften zwischen ihm und ebendiesem Staat als Geschäftspartner nicht gelten. Mit freiem Welthandel steht das kaum im Einklang.

11.4.5 Man wird den Eindruck nicht los, daß die Kryptologie zu Beginn des 3. Jahrtausends immer noch gern in *Black Chambers* gehalten wird. Die Staatsgewalt ist insofern undurchschaubar und klammert sich hier und da noch an Reste von Omnipotenz. Aber sie kann diese aus Gründen des Gleichgewichts auch nicht gänzlich aufgeben: Nicht nur bei den Großmächten, sondern auch bei den Mittelmächten wird es sich auf längere Sicht als notwendig erweisen, daß sich private und kommerzielle Kryptographie und Kryptanalyse mit den Erfordernissen der staatlichen Macht abfinden. Großbritannien, ein klassisches Land der Demokratie, gibt hier ein Beispiel. Wer seine eigene Sicherheit nicht beschützt, gibt auch die Sicherheit seiner Freunde preis. Andererseits lassen sich die Ansprüche der kommerziellen Seite nicht abtun.

Es wäre in den U.S.A. politisch kaum akzeptabel, wenn Patentanmeldungen für kryptographische Systeme durch den *Invention Secrecy Act* von 1940 oder den *National Security Act* von 1947 generell blockiert werden könnten. Gleichermaßen ist die Empfindlichkeit über den Schutz privater oder persönlicher Daten ein nicht zu übersehender politischer Faktor. In den U.S.A. konnte sich die Politik immer noch nicht über die Durchführung der inländischen Kontrolle entscheiden, wie sich durch das Aufsehen zeigte, das FIDNET (Federal Intrusion Detection Network) und CESA (Cyberspace Electronic Security Act) im Jahre 1999 erreichten.

11.4.6 Die fortschreitende Liberalisierung wurde 1997 durch internationale Organisationen wie OECD und EU in Gang gebracht. Im Dezember 1998 wurden im Zuge des Wassenaar-Abkommens (*Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*), dem 28 Staaten angehören, einige Richtlinien für einen ziemlich liberalen Export kryptographischer Güter erzielt. Insbesondere wurde der Export von 64-Bit-Chiffrieralgorithmen aus der staatlichen Überwachung durch die Mitgliedsstaaten des Wassenaar-Abkommens herausgenommen,

Am 16. September 1999 kündigte dann die Regierung der Vereinigten Staaten ihre Absicht weiterer Liberalisierung an, "*allowing the export and reexport of any encryption commodity or software to individuals, commercial firms, and other non-government end-users in all destinations*". Die neue Politik soll die Regeln für den U.S. Export von kryptographischen Gütern vereinfachen und beruht auf drei Grundsätzen: "*a technical review of encryption products in advance of sale, a streamlined post-export reporting system, and a process that permits the government to review exports of strong encryption to foreign governments.*" Das lindert die Schmerzen der amerikanischen Wirtschaft. "*Restrictions on terrorist-supporting states, their nationals and other sanctioned entities are not changed by this rule.*" Das mag das *U.S. Department of Justice* beruhigen. Insgesamt erwartet die U.S. Regierung daß "*the full range of national interests continue to be served by this new policy: supporting law enforcement and national security, protecting privacy, and promoting electronic commerce*".

Auf die vielversprechende Ankündigung folgten Taten. Am 12. Januar 2000 veröffentlichte das *Bureau of Export Administration* (BXA) das ungeduldig erwartete *interim final.* Firmen können nun uneingeschränkt Quell-Code zum internen Gebrauch auch über die Grenze weitergeben, lediglich eine Kopie ist an das BXA zu übersenden. Das Betriebssystem Windows 2000 kann damit auch außerhalb der U.S.A. mit 128-Bit-Schlüssellänge ausgeliefert werden. Nicht nur *Phil Zimmermann*, sondern die ganze U.S. Wirtschaft reagierte erleichtert. Europäische Produzenten von Krypto-Software sehen ihre bisherige starke Position nicht ernsthaft gefährdet und setzen auf Partnerschaft.

Kritiker der neuen Regelung sehen immer noch „ernste Defizite“ und meinen, „immer noch habe der Staat überall die Finger im Spiel“ (Holger Bleich). Insgesamt zeichnet sich derzeit aber ein Sieg der Vernunft ab.

11.4.7 Nach wie vor ist zu hoffen daß auch langfristig die Vernunft den Sieg davontragen nwird. Ziel der wissenschaftlichen Arbeit an kryptographischen Systemen für private und kommerzielle Kanäle muß daher weiterhin sein, unter realistischen Annahmen über die von Laien zu erwartenden Disziplinlosigkeiten untere Schranken für die Komplexität der unbefugten Entzifferung auf der Basis eines genau definierten Maschinentyps zu gewinnen. Das wird nicht leicht sein, ist aber eine lohnende Aufgabe, um dem Benutzer eines kryptographischen Systems ein garantiertes Maß an kryptanalytischer Sicherheit zu

geben. Offener Quell-Code ist dabei ein wesentliches Erfordernis, denn jedes Kryptosystem mit einem unpublizierten Algorithmus kann unerfreuliche Überraschungen in sich bergen.



Der Diskos von *Phaistos*, eine kretisch-minoische Tonscheibe (abgebildet ist die Seite A) von etwa 16 cm Durchmesser aus dem 17. Jhdt. v. Chr., ist in klarer Worttrennung mit Bildzeichen bedeckt. Eine überzeugende, allgemein akzeptierte Entzifferung scheint bisher nicht geglückt zu sein.
„Dem vereinzelten und kurzen Texte ist ohne weitere Anhaltspunkte kein Sinn abzugewinnen“ (*J. Friedrich*, 1954).

Farbtafel A

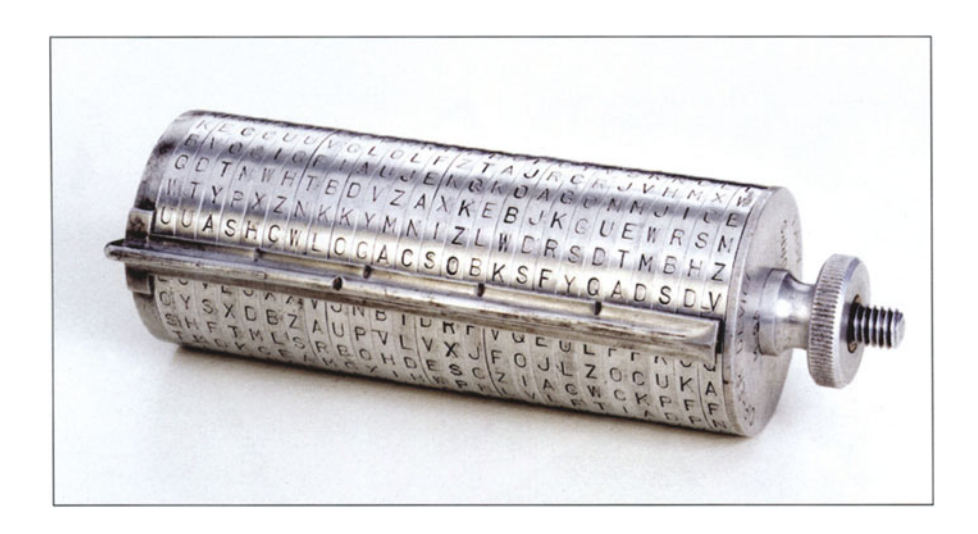


Farbtafel B Zwei Chiffrierscheiben, vermutlich aus dem 18./19. Jhdt. Die obere Scheibe enthält im Stil eines Nomenklators klartextseitig neben den Alphabetzeichen und einzelnen Silben auch häufig vorkommende Zeichengruppen; geheimtextseitig werden zweistellige Zahlen gebraucht.



‘Cryptograph’ von *Charles Wheatstone*, Gerät in Uhrenform, auf der Pariser Weltausstellung 1867 erstmals gezeigt. Polyalphabetisches Chiffriergerät; der Zeiger wird im Uhrzeigersinn auf den jeweils nächsten zu chiffrierenden Klartextbuchstaben weiterbewegt, dadurch wird die Scheibe mit den Chiffratbuchstaben Zug um Zug verdreht.

Farbtafel C



Farbtafel D Chiffriergerät M-94 der U.S. Army in zylindrischer Form mit 25 gravierten Aluminiumscheiben von 35 mm Durchmesser. Die M-94 geht auf die Vorbilder von *Jefferson* und *Bazeries* zurück. Sie wurde 1922 unter dem Einfluß von *Friedman* für den Truppendienst eingeführt und war bis etwa 1942 in der amerikanischen Armee weithin in Gebrauch.



Schiebergerät M-138-T4, eine frühe Variante des weitverbreiteten M-138-A, von der U.S. Army und der U.S. Navy im 2. Weltkrieg benutzt, auf einem Vorschlag von *Parker Hitt* 1914 beruhend. Die 25 entfernbaren Kartonstreifen waren numeriert und wurden in einer vorher verabredeten Reihenfolge gebraucht. Die Chiffrierung war kryptologisch der der M-94 äquivalent.

Farbtafel E



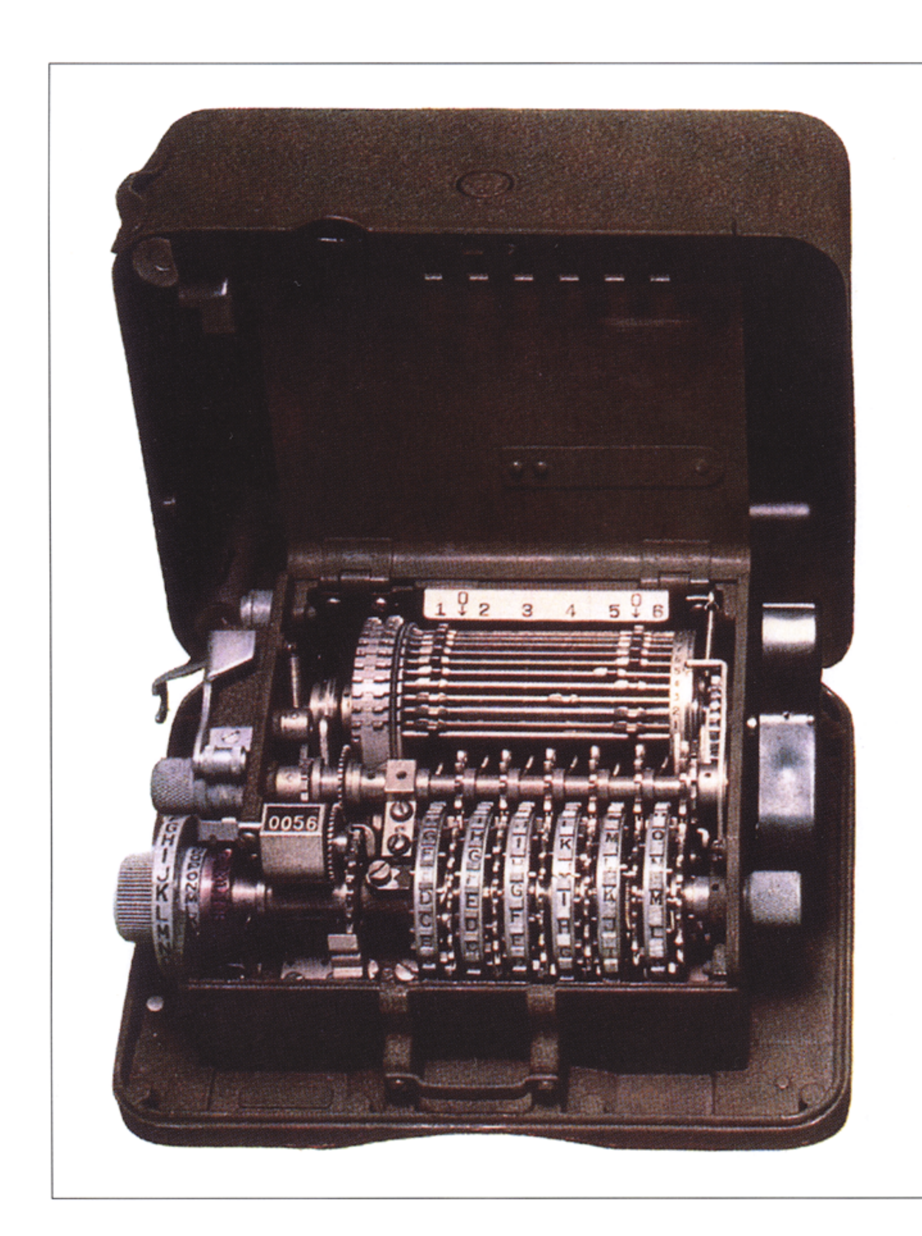


Farbtafel F Chiffriermaschine KRYHA, *Alexander von Kryha*, Berlin-Charlottenburg, um 1926. Polyalphabetische Chiffriermaschine mit festem periodischen Schlüssel der Länge 442. Eine unregelmäßige Fortschaltung der Chiffratscheibe geschieht durch ein Rad mit variierender Zähnezahl. Trotz ihrer kryptologischen Mängel wurde die hübsch aussehende Maschine in viele Länder verkauft.



Chiffriermaschine 'Hagelin Cryptographer' C-36, Aktiebolaget Cryptoteknik, Stockholm, 1936. Die Chiffrierung ist involutorisch (BEAUFORT-Substitutionen) und geschieht durch den von *Boris Hagelin* erfundenen Stangenkorb; die unregelmäßige Fortschaltung basiert auf der Verwendung von Schlüsselrädern unterschiedlicher Teilung, nämlich mit 17-, 19-, 21-, 23- und 25-Teilung, was eine Periodenlänge ('Schlüssellänge') von 3 900 225 ergibt. Für rein mechanisch arbeitende Maschinen bedeutete dies eine Pionierleistung.

Farbtafel G



Farbtafel H M-209, eine verbesserte C-36, wurde im 2. Weltkrieg bei Smith-Corona in Lizenz für die U.S. Army in 140 000 Stück gebaut. Durch zusätzliches 6. Schlüsselrad mit 26-Teilung stieg die Periode auf 101 405 950. Wenn die Kurbel gedreht wurde, verschoben die Schlüsselräder die Stangen in dem zylindrischen Korb; dadurch wurde das Druckrad auf den chiffrierten Buchstaben eingestellt.



Rotor-Chiffriermaschine ENIGMA nach der Erfindung von *Arthur Scherbius* 1919, mit Glühlampenanzeige; 4-Rotoren-Ausführung M4 für die Marine, 1944. Rotor-Chiffriermaschine mit dünner Umkehrwalze und insgesamt zehn Rotoren. Drei der vier Rotoren in der Maschine konnten aus den acht Rotoren I bis VIII ausgewählt werden, die vierte (ganz links) aus den sogenannten 'Griechenwalzen' β und γ. Die Einführung der 4-Rotoren-ENIGMA unterband das Mitlesen durch die Briten vom 1. 2. 1942 bis Dezember 1942.

Farbtafel I

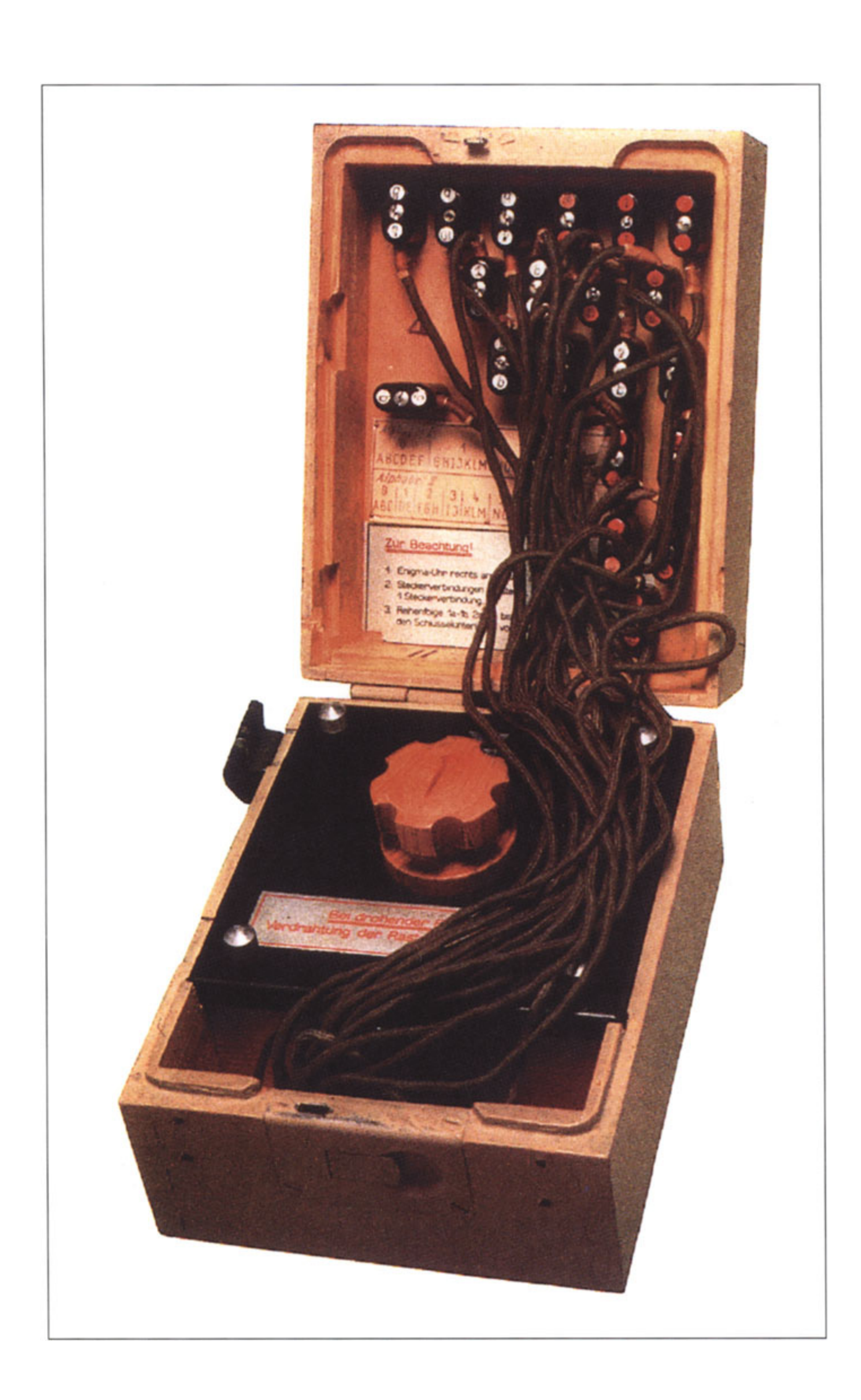


Farbtafel K Rotoren der ENIGMA: Die innere Verschaltung hat 26 galvanische Verbindungen der 26 Kontakte auf der einen Seite mit ebenso vielen auf der anderen Seite.
Oben: Rotor I mit sichtbarem Einstellring.
Unten: Rotor VIII mit zwei Nuten.

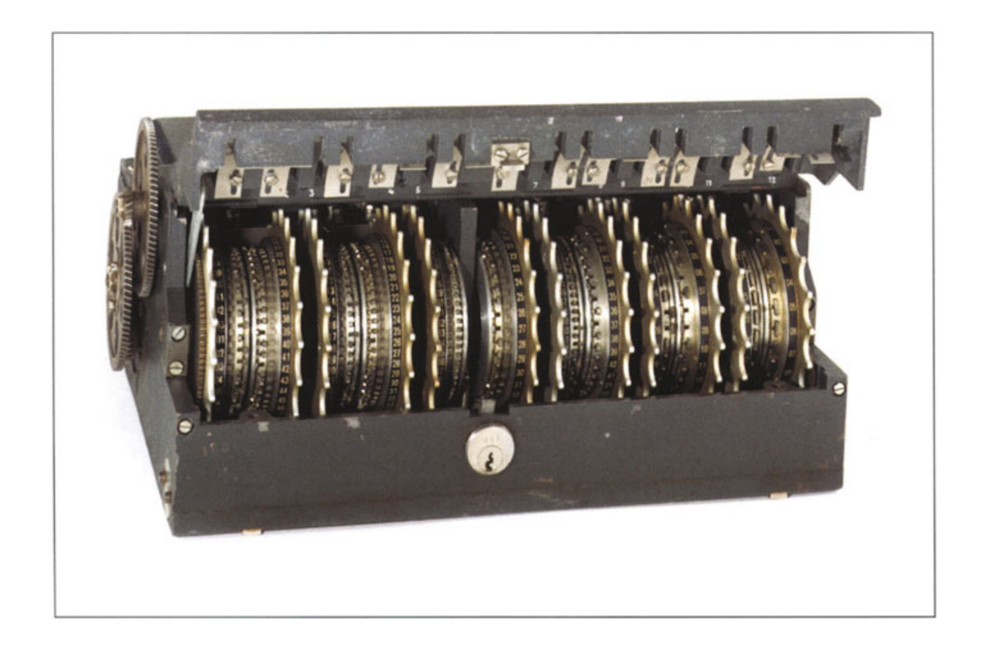


Farbtafel L

Die britische Chiffriermaschine TYPEX war eine wesentlich verbesserte Kopie der Wehrmachts-ENIGMA mit drei Rotoren; sie hatte zwei zusätzliche, nicht fortgeschaltete Rotoren, die ein Eindringen in die Chiffrierung wesentlich erschwerten. TYPEX war in britischen militärischen Nachrichtenverbindungen eingesetzt, diente aber auch zur mechanischen Entzifferung deutscher ENIGMA-Sprüche, deren Schlüssel aufgedeckt war. Die Abbildung zeigt eine TYPEX Mark III, Serial No. 376.



Zur Beachtung!



Farbtafel N

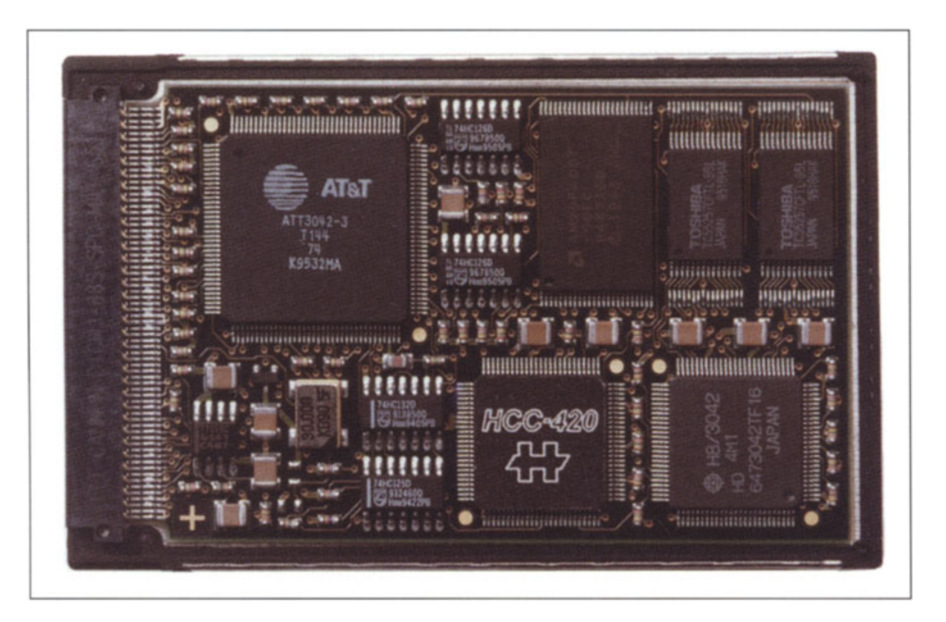
Chiffrierfernschreibmaschine „Schlüsselzusatz“ Lorenz SZ 42, C. Lorenz AG, Berlin, um 1943. Chiffriermaschine für Fernschreibzeichen, britischer Deckname ‘Tunny’. Eingesetzt in der Heeresführung bis hinab zu Armeehauptquartieren. Zwölf Walzen mit 43-, 47-, 51-, 53-, 59-, 37-, 61-, 41-, 31-, 29-, 26-, 23-Teilung und unregelmäßig verteilten Stiften erzeugen einen Schlüssel mit hoher Periode. Fünf Walzenpaare steuern Vernam-Substitutionen des 5-Bit-Codes; zwei Walzen dienen lediglich der unregelmäßigen Fortschaltung. Die Chiffrierung der SZ 42 wurde von den Briten unter Einsatz der COLOSSUS-Anlagen gebrochen, die zu den ersten elektronischen Großrechenanlagen zählen.

Farbtafel M

Die *Uhr box* (wie sie auf alliierter Seite genannt wurde) diente dazu, die Steckerbrett-Verbindungen der ENIGMA durch eine nicht-involutorische Substitution zu ersetzen, die außerdem durch Drehen des Einstellknopfes auf eine von 40 Positionen leicht geändert werden konnte (vermutlich jede Stunde). Trotz der zusätzlichen Sicherheit, die sie bot, wurde sie wenig eingesetzt.

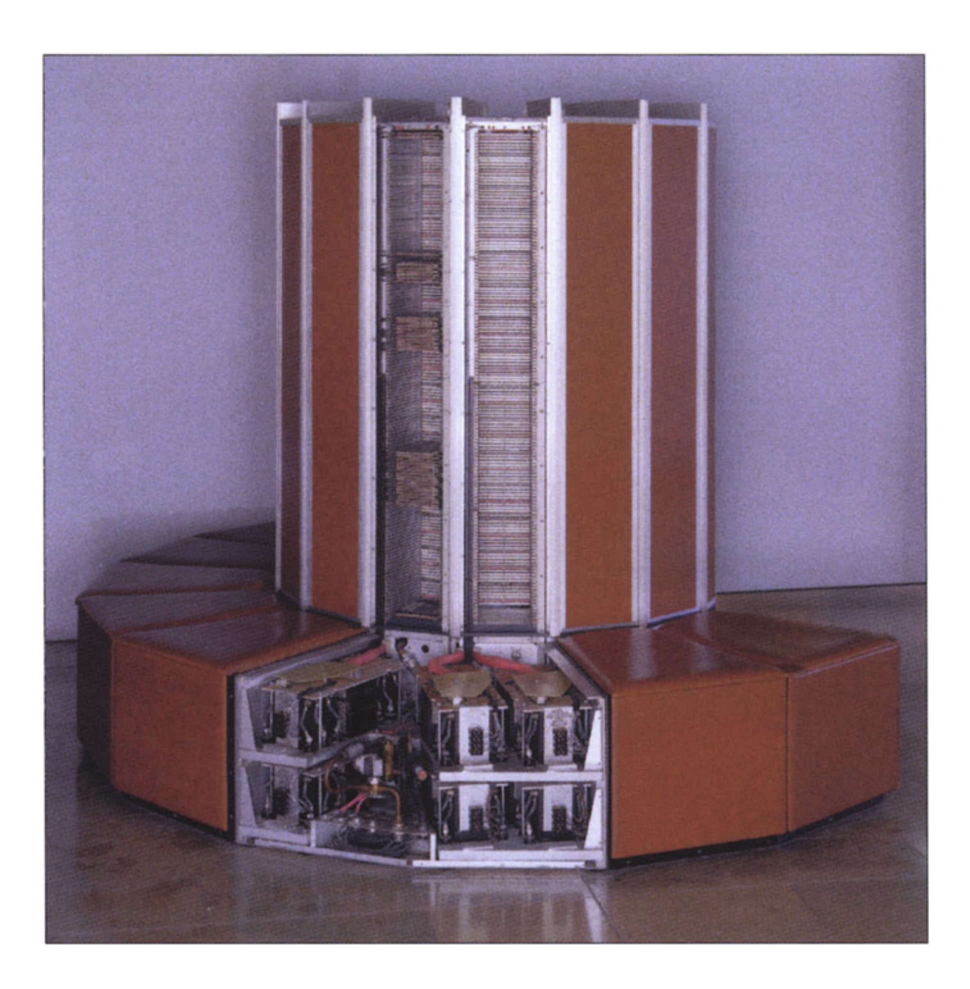


Farbtafel O Individueller Schlüssel für einmaligen Gebrauch. Das Blatt aus einem Abreißblock ist klein genug, um in die Handfläche zu passen. Die verwendeten Ziffern-Typen sind von der Art, wie sie auf russischen Schreibmaschinen vorkommen.



'Crypto board', gefertigt von der Crypto AG, Zug, Schweiz (1996). Kryptosystem zur Verwendung bei einzelnen Rechnern und in Rechnernetzen zur Geheimhaltung und Sicherung gegen Fälschung von Daten, mit Zugangskontrolle und Schutz gegen Computer-Viren. Die sehr zuverlässige *hardware* des Kryptosystems hat eine sehr hohe mittlere fehlerfreie Zeit und kann ohne Batterien gelagert werden.

Farbtafel P



Farbtafel Q CRAY-1 S (1979). Die Höchstgeschwindigkeitsrechner CRAY entstanden aus der von *Seymour R. Cray* (1928–1996) für kryptanalytische Aufgaben entworfenen, 1976 betriebsbereiten CRAY-1, die 8 Mio. $ teuer war. Zivile Versionen mit gewissen Beschränkungen seit 1979 im Handel; Weiterentwicklung zu leistungsfähigsten Universalrechnern, mit parallel arbeitenden Funktionseinheiten und überschnellen speziell gekühlten Schaltkreisen, die eine sehr kompakte Technologie erfordern: CRAY-1 S, CRAY-2, CRAY X-MP, CRAY Y-MP, CRAY C90, CRAY J90 bis hin zu CRAY T90, deren Konfiguration T932 mit 32 Prozessoren ausgestattet ist. Eine massiv parallele Linie wurde mit dem Modell CRAY T3D eröffnet, das nächste Modell CRAY T3E (Juli 1996) hat bis zu 2048 flüssigkeitsgekühlte Prozessorchips des Typs DEC Alpha EV-5 (21164) mit 600 Megaflops – in der Spitze eine Rechenleistung von 1.2 Teraflops (1998: T3E-1200E 2.4 Teraflops).

Teil II: Kryptanalyse

≪Il ne faut alors ni se buter,
ni se rebuter,
et faire comme en politique:
changer son fusil d'épaule.≫

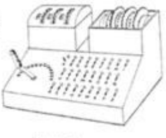
(„Man darf sich daher weder verrennen
noch abschrecken lassen
und muß es machen wie in der Politik:
umschwenken.")

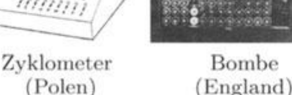
Étienne Bazeries, 1901



Étienne Bazeries
(1846–1931)

Die Maschinerie







Zyklometer (Polen) Bombe (England) Colossus (England)

Charles Babbage bekennt, daß ihn manchmal die Entzifferung in den Bann geschlagen und über Gebühr beschäftigt hat. *Bazeries'* Zitat warnt mit gallischem Charme davor, die Systematik der in diesem zweiten Teil behandelten kryptanalytischen Methoden zu überschätzen.[1]

Von der einfachen, aber im allgemeinen nicht zu bewältigenden Ausschöpfung abgesehen, beruhen sie auf inneren und auch durch raffinierte Chiffrierung nur schwer ausrottbaren Eigenschaften der Sprache. Für eine systematische Behandlung werden die Invarianten der kryptologischen Verfahren festgestellt und herangezogen. Mustererkennung einerseits, Häufigkeitserkennung andererseits liefert Invarianten monoalphabetischer (monographischer oder polygraphischer) Chiffrierungen. Aber selbst polyalphabetische Chiffrierung läßt einen gewissen sprachlich-statistischen Parameter, genannt Kappa, invariant. Damit gelingt die Zurückführung polyalphabetischer Chiffrierung mit nicht zu langer Periode auf monoalphabetische Chiffrierung. Die Transposition fällt ganz aus diesem methodischen Rahmen, hier werden Kontakthäufigkeiten herangezogen.

Nach *William F. Friedman* verlangt Kryptanalyse die Feststellung der verwendeten Sprache, des allgemeinen Kryptosystems, des spezifischen Schlüssels und des Klartextes; gewöhnlich in dieser Reihenfolge. Dabei kommt es sehr darauf an, die richtigen Mittel an der richtigen Stelle in der richtigen Weise einzusetzen. Ein anonymer britischer Offizier drückte es 1918 so aus: "*The would-be solver will need a dogged obstinacy, which however must not render him incapable of discarding a supposed clue.*"

Es muß auch darauf hingewiesen werden, daß aktives kryptanalytisches Arbeiten sowohl gegen staatliche als auch gegen kommerzielle Nachrichtenwege in der Regel mit Strafe bedroht ist. Da aber nur aus der Kenntnis kryptanalytischer Methoden Rückschlüsse auf die sichere Verwendung kryptographischer Verfahren, insbesondere zur Vermeidung einer *complication illusoire*, zu ziehen sind, werden wir uns aus wissenschaftlichen Gründen ungestraft mit der Kryptanalyse beschäftigen dürfen.

---

[1] Die erste systematische Sammlung von Faustregeln zur Kryptanalyse verfaßte 1474 in Pavia *Cicco Simonetta*, Sekretär der Herzöge von Sforza.

Kryptanalyse ist häufig nicht nur eine Frage des Materialaufwands, sondern auch der verfügbaren Zeit. Viele Nachrichten sind, wenn sie erst veraltet sind, nichts mehr wert, und auf manchen Gebieten veralten Nachrichten sehr schnell. Dazu *Patrick Beesly* (Very special intelligence, London 1977): "*It should, however, be emphasized that cryptanalysis must be swift to be of real operational use.* Und *W. F. Friedman* stellte fest: "*The best that can be expected is that the degree of security be great enough to delay solution by the enemy for such a length of time that when the solution is finally reached, the information thus obtained has lost all its ... value.*"

Auch Chiffrierhilfsmittel sind nur so lange von unmittelbarem Wert, als sie in Gebrauch sind. Auf deutscher Seite wurden im 1. Weltkrieg 1917 die für die vorderste Front bestimmten Codebücher alle vierzehn Tage gewechselt, und 1918 eine Überschlüsselungstafel („Geheimklappe") jeden Tag. Da konnte auch mal ein Codebuch oder eine Überschlüsselungstafel in falsche Hände fallen. Trotzdem, es verraten auch veraltete Chiffrierhilfsmittel zu viel, als daß man mit ihnen sorglos umgehen könnte.

Die Anforderungen an eine geglückte unbefugte Entzifferung schwanken je nach der Situation, von der Rekonstruktion von 90% des Klartextes (*Meyer-Matyas*) bis zur vollständigen Bloßlegung des Chiffriersystems und der Schlüssel (*Rohrbach*).

Kryptanalyse baut zu einem guten Teil auf Chiffrierfehlern auf. Daß der unbefugte Entzifferer stets auf solche hoffen kann, hat *Luigi Sacco* sarkastisch so formuliert: "*Les chiffreurs se chargent suffisamment d'aider l'ennemi.*" [Die Chiffrierer bemühen sich hinreichend, dem Feind zu helfen.]

Asymmetrische Chiffriersysteme, die öffentliche Chiffrierschlüssel ("*public key*") erlauben, signalisieren eine Öffnung der Kryptographie ("*public cryptography*"), die auch eine Öffnung der Kryptanalyse nach sich zieht – wenn auch die kryptologischen Dienste der Staaten diese Seite der *public cryptography* eher mit Zurückhaltung sehen. Daß sie sich nicht zu sehr der Volksaufklärung verpflichtet sehen, ist verständlich. Im Hinblick auf die Betriebsmodi von DES (9.6.3) haben Umfragen, wie *Philip Zimmermann* berichtet, ergeben, daß "... *the authors of a number of* [these encryption packages] *say they've never heard of CBC or CFB mode. The very fact that they haven't even learned enough cryptography to know these elementary concepts is not reassuring.*" Die Kryptanalyse ist nicht in Gefahr, auszutrocknen.

Kryptanalyse ist auch bereits auf dem freien Markt. Die Firma Access Data Recovery (87 East 600 South, Orem, Utah 84058, USA) – und sie ist nicht die einzige – verkauft für einige hundert Dollar ein von *Eric Thompson* entwickeltes Programm, das die eingebauten Chiffrierungen von WordPerfect, Lotus 1-2-3, MS Excel, Symphony, Quattro Pro, Paradox und MS Word 2.0 überwindet, und zwar nicht durch exhaustives Erraten von Paßwörtern, sondern durch echt kryptanalytische Methoden. Manche Leute kaufen oder benutzen es, wenn sie ihr Paßwort vergessen haben, und auch Polizeibehörden profitieren davon, wenn sie beschlagnahmte Daten lesen wollen.

12 Ausschöpfung der kombinatorischen Komplexität

Die Mächtigkeit eines Verfahrens, d.h. einer Klasse von Chiffrierungen – ihr entspricht die Anzahl von dazugehörigen Schlüsseln – ist ein Maß für die **kombinatorische Komplexität** der Chiffrierung. Für die Sicherheit gegen unbefugte Entschlüsselung gibt sie eine *obere Schranke* an, sie mißt den Arbeitsaufwand eines Exhaustionsverfahrens bei bekanntem Verfahren (*Shannon*s Maxime: „Der Feind kennt das benutzte System“).

Wir werden häufig von der Stirling'schen Formel[1]

$$n! \asymp (n/e)^n \sqrt{2\pi n} \cdot (1 + \tfrac{1}{12n} + \tfrac{1}{288n^2}) = \sqrt{2\pi e}(n/e)^{n+\frac{1}{2}} \cdot (1 + \tfrac{1}{12n} + \tfrac{1}{288n^2})$$

mit den Zahlwerten

$$\sqrt{2\pi} = 2.506\,628\,275\ldots\ ,$$
$$e = 2.718281828\ldots\ ,$$
$$\sqrt{2\pi e} = 4.132\,731\,353\ldots$$

Gebrauch machen bzw. von ihrer logarithmischen Form[2]

$$\mathrm{ld}\, n! \asymp (n + \tfrac{1}{2})\ (\mathrm{ld}\, n - \mathrm{ld}\, e) + \tfrac{1}{2}(\mathrm{ld}\, \pi + \mathrm{ld}\, e + 1) + \tfrac{1}{12n} + \tfrac{1}{288n^2}$$

mit den Zahlwerten

$$\mathrm{ld}\, e = 1.442\,695\,041\ldots\ ,$$
$$\tfrac{1}{2}(\mathrm{ld}\, \pi + \mathrm{ld}\, e + 1) = 2.047\,095\,586\ldots\ .$$

$|\,V\,|$, die Mächtigkeit des Alphabets, wird mit N abgekürzt.

Z bezeichnet die Mächtigkeit des Verfahrens.

Im folgenden sind für einige Verfahren die Werte von Z als Maße für **kombinatorischen Komplexitäten** zusammengestellt.

$\mathrm{ld}\, Z$, die Information des Verfahrens S, wird in [bit] gemessen.

${}^{10}\log Z$ wird in [ban] gemessen, eine von Turing eingeführte Einheit, mit der praktischen Einheit $1\,[\text{deciban}] = 0.1/{}^{10}\log 2\ [\text{bit}] \approx 0.332\ [\text{bit}]$.

---

1 $26! = 403\,291\,461\,126\,605\,635\,584\,000\,000 = 2^{23} \cdot 3^{10} \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23$

2 $\mathrm{ld}\, x$ bezeichnet den Logarithmus zur Basis 2: $\mathrm{ld}\, x = \ln\, x/\ln\, 2 = \log\, x/\log\, 2$.

12.1 Monoalphabetische einfache Chiffrierungen

Einfache Substitutionen sind monographisch. Wenn wir Homophone und Blender außer acht lassen, können uns auf Permutationen (3.2) beschränken.

12.1.1 Einfache Substitutionen allgemein (Spezialfall $n = 1$ von 12.2.1)

12.1.1.1 (Einfache Substitutionen)

Permutationen $V \longleftrightarrow V$ haben die selbe Mächtigkeit wie eineindeutige Abbildungen (homophonfrei) von V *in* $W^{(m)}$, unabhängig von W und m:

$$Z = N! \asymp \sqrt{2\pi e}\left(\frac{N}{e}\right)^{N+\frac{1}{2}} = 4.13 \cdot \left(\frac{N}{e}\right)^{N+\frac{1}{2}}$$

$$\mathrm{ld}\, Z \asymp \left(N + \frac{1}{2}\right) \cdot (\mathrm{ld}\, N - 1.44) + 2.05$$

Für $N = 26$ ist $Z \approx 4.03 \cdot 10^{26}$, $\mathrm{ld}\, Z \approx 88.38$ [bit], $\log Z \approx 266.06$ [deziban].

12.1.1.2 (Voll zyklische einfache Substitutionen, vgl. 3.2.3)

Permutationen $V \overset{N}{\longleftrightarrow} V$ mit genau einer Zusammenhangskomponente, von der maximalen Ordnung N:

$$Z = (N-1)! \asymp \sqrt{2\pi e}\left(\frac{N-1}{e}\right)^{N-\frac{1}{2}} = 4.13 \cdot \left(\frac{N-1}{e}\right)^{N-\frac{1}{2}}$$

$$\mathrm{ld}\, Z \asymp \left(N - \frac{1}{2}\right) \cdot (\mathrm{ld}\,(N-1) - 1.44) + 2.05$$

Für $N = 26$ ist $Z \approx 1.55 \cdot 10^{25}$, $\mathrm{ld}\, Z \approx 83.68$ [bit], $\log Z \approx 251.91$ [deziban].

12.1.1.3 (Echt involutorische einfache Substitutionen, vgl. 3.2.1)

Für eine echt involutorische Permutation $V \overset{2}{\longleftrightarrow} V$ muß N gerade sein, $N = 2\nu$. Sie ist von der Ordnung 2:

$$Z = (N-1)!! \overset{def}{=} (N-1)(N-3)(N-5)\ldots \cdot 5 \cdot 3 \cdot 1 \asymp \sqrt{2} \cdot \left(\frac{N}{e}\right)^{\frac{N}{2}}$$

$$\mathrm{ld}\, Z \asymp \frac{N}{2} \cdot (\mathrm{ld}\, N - 1.44) + \frac{1}{2}$$

Für $N = 26$ ist $Z \approx 7.91 \cdot 10^{12}$, $\mathrm{ld}\, Z \approx 42.85$ [bit], $\log Z \approx 128.98$ [deziban].

12.1.2 Dezimierte Alphabete (Spezialfall $n = 1$ von 12.2.2)

Sie setzen eine lineare Alphabetordnung voraus und nehmen jeweils (vgl. 5.6) das q-te Element *modulo N* (*Sinkov*: *'decimation by q'*).

$$Z = \varphi(N) \quad \text{, wo } \varphi \text{ die Eulersche Funktion ist (vgl. 5.6)}$$

$$\mathrm{ld}\, Z = \mathrm{ld}\, N + \textstyle\sum_{\mu=1}^{k} \mathrm{ld}\, \rho(p_\mu, 1) \quad \text{(vgl. 12.2.2)}$$

Für $N = 26$ ist $Z = 12$ (vgl. 5.5, Tabelle 1b),
$\mathrm{ld}\, Z \approx 3.58$ [bit], $\log Z \approx 10.79$ [deziban].

	Z	$\mathrm{ld}\,Z$
12.2.1 Substitutionen allgemein	$(26^n)\,!$	$(26^n + \frac{1}{2})(4.70\,n - 1.44) + 2.05$
12.2.2 Homogene lineare Substitutionen	$0.265 \cdot 26^{n^2}$	$4.70\,n^2 - 1.916$
12.2.3 Additionen	26^n	$4.70\,n$
12.2.4 Transpositionen	$n!$	$(n + \frac{1}{2})(\mathrm{ld}\,n - 1.44) + 2.05$

Tabelle 3. Komplexität monoalphabetischer (polygraphischer) Chiffrierschritte

12.1.3 CAESAR-Additionen (Spezialfall $n=1$ von 12.2.3)
Auch sie setzen eine lineare Alphabetordnung voraus. CAESAR-Addition $V \overset{+}{\longleftrightarrow} V$, eine reine Verschiebung, ist der monoalphabetische Spezialfall einer VIGENÈRE-Substitution (7.4.1).

$$Z = N$$
$$\mathrm{ld}\,Z = \mathrm{ld}\,N$$

Für $N=26$ ist $Z = 26$, $\mathrm{ld}\,Z \approx 4.70$ [bit], $\log Z \approx 14.15$ [deziban].

12.2 Monoalphabetische polygraphische Chiffrierungen

Für polygraphische Substitutionen hängt die kombinatorische Komplexität auch von der Chiffrierbreite n ab.

12.2.1 Polygraphische Substitutionen allgemein

Permutationen $V^n \longleftrightarrow V^n$ haben die selbe Komplexität wie eineindeutige Abbildungen (homophonfrei) von V^n *in* $W^{(m)}$, unabhängig von W und m.

$$Z = (N^n)!$$
$$\mathrm{ld}\,Z \asymp \left(N^n + \frac{1}{2}\right)(n \cdot \mathrm{ld}\,N - 1.44) + 2.05$$

Für $N=26$ ist $Z = (26^n)!$, $\mathrm{ld}\,Z \approx (26^n + \frac{1}{2})(4.70\,n - 1.44) + 2.05$;

Bigramm-Permutationen: $Z \approx 1.88 \cdot 10^{1621}$, $\mathrm{ld}\,Z \approx 5.39 \cdot 10^3$ [bit]
Trigramm-Permutationen: $Z \approx 1.19 \cdot 10^{66978}$, $\mathrm{ld}\,Z \approx 2.23 \cdot 10^5$ [bit]
Tetragramm-Permutationen: $Z \approx 4.82 \cdot 10^{2388104}$, $\mathrm{ld}\,Z \approx 7.93 \cdot 10^6$ [bit]

PLAYFAIR-Permutationen haben die selbe Komplexität wie einfache zyklische Permutationen mit $N=25$:

$$Z = 25!/(5\cdot 5) \approx 6.20 \cdot 10^{23}\ , \mathrm{ld}\,Z \approx 79.04 \text{ [bit]}, \log Z \approx 237.93 \text{ [deziban]}.$$

ld Z				
$n=1$	$n=4$	$n=16$	$n=64$	$n=256$
$8.84 \cdot 10^1$	$7.93 \cdot 10^6$	$3.22 \cdot 10^{24}$	$1.08 \cdot 10^{93}$	$2.07 \cdot 10^{365}$
3.58	73.29	$1.20 \cdot 10^3$	$1.93 \cdot 10^4$	$3.08 \cdot 10^5$
4.70	18.80	75.21	300.83	1203.31
	4.58	44.25	296.00	1684.00

für $N=26$ in Abhängigkeit von der Chiffrierbreite n

12.2.2 Polygraphische homogene lineare Substitutionen (*Hill*)

Sie setzen ebenfalls eine lineare Alphabetordnung voraus. Nach 5.2.3 ist

$$Z = N^{n^2} \cdot \rho(N,n) \quad , \quad \text{wo für } N = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$$
$$\rho(N,n) = \rho(p_1,n)\rho(p_2,n)\dots\rho(p_k,n).$$
$$\operatorname{ld} Z = n^2 \operatorname{ld} N + \textstyle\sum_{\mu=1}^{k} \operatorname{ld} \rho(p_\mu,n) \ .$$

Für große n findet man Näherungswerte für $\rho(p,n)$ in 5.2.3;
für große n und nicht zu kleine p ist mit $\operatorname{ld} e \approx 1.44$

$$\operatorname{ld} \rho(p,n) \approx 1.44 \ / \ (\tfrac{3}{2} - p) \, .$$

Für $N=26$ und große n ist $\rho(2,n) \approx 0.289$ und $\rho(13,n) \approx 0.917$, also ist $\rho(26,n) \approx 0.289 \cdot 0.917 = 0.265$, $\operatorname{ld} \rho(26,n) \approx 1.92$; wir bekommen:

Für $N=26$ und große n ist
$Z \approx 0.265 \cdot 26^{n^2}$, $\operatorname{ld} Z \approx 4.70\, n^2 - 1.92$ [bit] , $\log Z \approx 14.15\, n^2 - 5.78$ [deziban] .

12.2.3 Polygraphische Additionen

Reine Verschiebungen als Spezialfall der inhomogenen linearen Substitution sind polygraphische CAESAR-Additionen $V^n \overset{+}{\leftrightarrow} V^n$ der Chiffrierbreite n.

$$Z = N^n \ , \quad \operatorname{ld} Z = n \operatorname{ld} N$$

Für $N=26$ ist $Z = 26^n$, $\operatorname{ld} Z \approx 4.70 \cdot n$ [bit], $\log Z \approx 14.15 \cdot n$ [deziban] .

12.2.4 Transpositionen

Transpositionen der Breite n reihen sich etwas künstlich unter lineare Substitutionen ein, wenn man sich auf solche beschränkt, deren Matrix eine Permutationsmatrix ist. Die Komplexität ist unabhängig von N .

$$Z = n\,!$$

$$\operatorname{ld} Z = (n + \tfrac{1}{2})(\operatorname{ld} n - 1.44) + 2.05$$

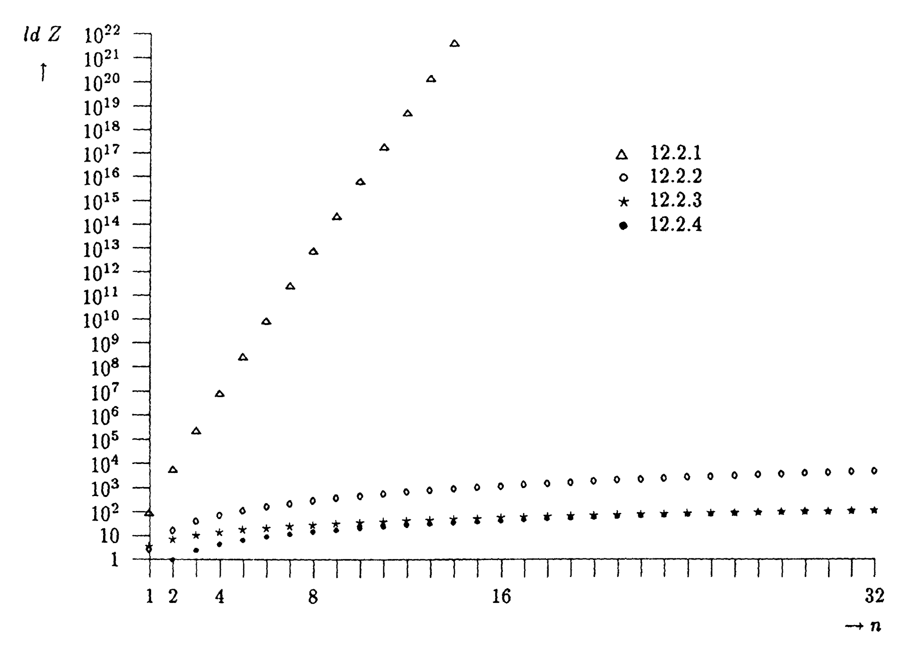


Abb. 80. Kombinatorische Komplexität polygraphischer Substitutionen der Breite n für $N=26$

Man beachte, daß eine Blocktransposition der Breite n zwar polygraphisch, aber monoalphabetisch ist – auch wenn irreführenderweise n manchmal als ‚Periode' bezeichnet wird.

12.2.5 Zusammenfassung über monoalphabetische Chiffrierungen

Eine tabellarische Zusammenstellung der Komplexitäten monoalphabetischer (polygraphischer) Chiffrierverfahren zeigt Tabelle 3. Den Verlauf gibt Abb. 80 graphisch wieder. Man beachte, daß die Komplexität der Transposition die der Addition, d.h. der polygraphischen CAESAR-Addition ungefähr bei $n = N \cdot e$ überholt (für $N=26$ genau bei $n=68$ mit $\operatorname{ld} Z \approx 320$).

Transposition erreicht erst bei $n=26$ einfache (Monogramm-)Permutation;
lineare Substitution erreicht bei $n=\ 4$ einfache (Monogramm-)Permutation,
bei $n=32$ Bigramm-Permutation.

Addition (polygraphische CAESAR-Addition) wird ab $n=2$ von homogener linearer Substitution übertroffen.

12.3 Polyalphabetische Chiffrierungen

Die allgemeine polyalphabetische (periodische) Chiffrierung mit d Alphabeten hat als (maximale) kombinatorische Komplexität das Produkt der Komplexitäten der einzelnen Alphabete. Für den uniformen Fall von d Alphabeten der gleichen Bauart ist das die d-te Potenz der Komplexität des Alphabets.

12.3.1 PERMUTE-Schritte mit Periode d

$$Z = (N\,!)^d$$

$$\mathrm{ld}\, Z = d \cdot ((N - \frac{1}{2})\,(\mathrm{ld}\, N - 1.44) + 2.05)$$

Für $N=26$ ist $Z = (4.03 \cdot 10^{26})^d$, $\mathrm{ld}\, Z = 88.382 \cdot d$ [bit] .

12.3.2 MULTIPLEX-Schritte mit Periode d

$$Z = ((N-1)\,!)^d$$

$$\mathrm{ld}\, Z = d \cdot ((N - \frac{1}{2})\,(\mathrm{ld}\,(N-1) - 1.44) + 2.05)$$

Für $N=26$ ist $Z = (1.55 \cdot 10^{25})^d$, $\mathrm{ld}\, Z = 83.681 \cdot d$ [bit] .

12.3.3 ALBERTI-Schritte mit Periode d

$$Z = (N-1)!\, N^d$$

$$\mathrm{ld}\, Z = d \cdot \mathrm{ld}\, N + (N - \frac{1}{2})(\mathrm{ld}\,(N-1) - 1.44) + 2.05$$

Für $N=26$ ist $Z = 1.55 \cdot 10^{25} \cdot 26^d$, $\mathrm{ld}\, Z \approx 4.70 \cdot d + 83.682$ [bit] .

12.3.4 VIGENÈRE- oder BEAUFORT-Schritte mit Periode d

$$Z = N^d$$
$$\mathrm{ld}\, Z = d\, \mathrm{ld}\, N$$

Für $N=26$ ist $Z = 26^d$, $\mathrm{ld}\, Z \approx 4.70 \cdot d$ [bit] .

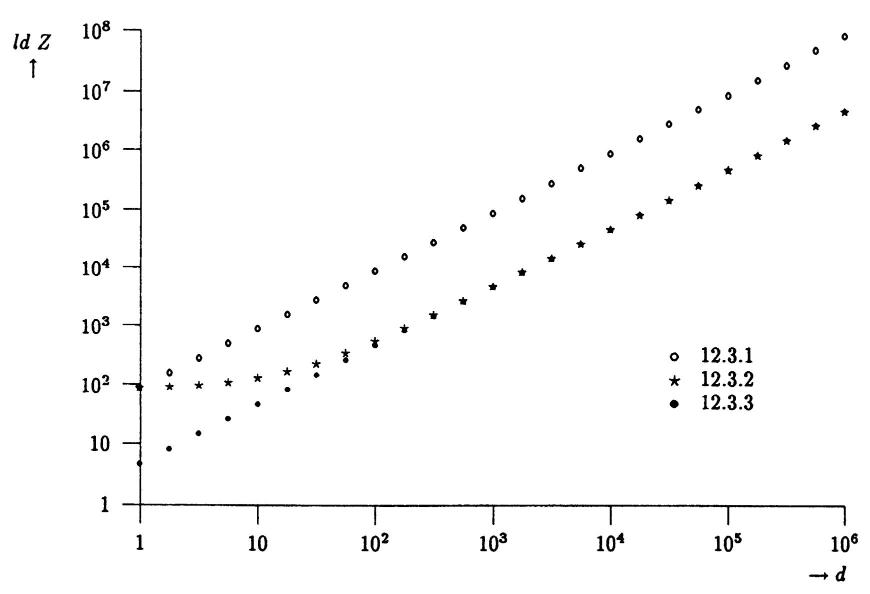


Abb. 81. Kombinatorische Komplexität polyalphabetischer Chiffrierungen der Periode d für $N=26$

	Z	$\operatorname{ld} Z$
12.3.1 PERMUTE-Substitutionen	$(26!)^d$	$88.38 \cdot d$
12.3.2 MULTIPLEX-Substitutionen	$(25!)^d$	$83.68 \cdot d$
12.3.3 ALBERTI-Substitutionen	$25!\,26^d$	$4.70 \cdot d + 83.68$
12.3.4 VIGENÈRE-Substitutionen	26^d	$4.70 \cdot d$

Tabelle 4. Komplexität polyalphabetischer (monographischer) Chiffrierverfahren

12.3.5 Zusammenfassung über polyalphabetische Chiffrierungen

Eine tabellarische Zusammenstellung der Komplexitäten zeigt Tabelle 4. Den Verlauf gibt Abb. 81 graphisch wieder.

Man beachte, daß VIGENÈRE-Substitutionen für $d \approx N + \frac{1}{2} - \frac{N - \ln 2\pi}{\ln N}$ (d.h., im Fall $N = 26$, für $d = 19$; im Fall $N = 26^2$, für $d = 573$) mit der *monoalphabetischen* einfachen Chiffrierung gleichziehen.

MULTIPLEX-Substitutionen ziehen mit monoalphabetischer n-gramm-Permutation gleich für $d \approx n \cdot N^{n-1}$, im Fall $N = 26$ und $n = 2$ genauer für $d = 55$.

Die Komplexität der VIGENÈRE- oder BEAUFORT-Verfahren mit Periode h und der Addition (d.h. der polygraphischen CAESAR-Addition) mit der Breite h stimmen überein [3].

12.4 Allgemeine Bemerkungen

Bei der Untersuchung der kombinatorischen Komplexität ist zu beachten, daß die gesamte Verfahrensklasse betrachtet wird. In der Praxis wird der unbefugte Entzifferer oft von den Umständen bestimmte Einschränkungen finden.

12.4.1 So ist der Zylinder von *Jefferson* und *Bazeries* ohne Kenntnis der Scheiben als MULTIPLEX-Verfahren aufzufassen, mit Kenntnis der Scheiben (Grundsatz: Ein Gerät kann in gegnerische Hände fallen[4]) jedoch nur mehr als Transposition. Für $d = 25$ (M-94) bedeutet das einen Rückgang von $Z = (26!)^{25} \approx 10^{665}$ auf $Z = 25! \approx 1.55 \cdot 10^{25}$, oder von $\operatorname{ld} Z \approx 2209$ auf $\operatorname{ld} Z \approx 83.7$. Ähnlich, wenn auch weniger drastisch, bei *Alberti*s Scheibe: Wenn sie in gegnerische Hände fällt, reduziert sich das ALBERTI-Verfahren zum VIGENÈRE-Verfahren; Z geht von $(N!) \cdot N^{d-1}$ auf N^d zurück, oder für $N = 26$, $\operatorname{ld} Z$ von $4.70 \cdot d + 83.68$ auf $4.70 \cdot d$.

[3] Für $N = 10$ kann man dazu ein h-stelliges Addierwerk benützen, dessen Übertragseinrichtung man im ersten Fall ausgebaut hat, im zweiten Fall nicht (vgl. 5.7 und 8.3.3).

[4] Regel Nr. 3 von 11.2.3. *Bazeries* erfand sein Gerät 1891, acht Jahre nachdem *Kerckhoffs* 1883 seine Maxime publiziert hatte.

ld Z				
$d=1$	$d=10$	$d=100$	$d=1000$	$d=10000$
88.38	883.82	8838.20	88381.95	883819.53
83.68	836.82	8368.15	83681.51	836815.36
88.38	130.69	553.73	4784.12	47088.08
4.70	47.00	470.04	4700.44	47004.40

für $N = 26$ in Abhängigkeit von der Anzahl d der Alphabete

12.4.2 Man beachte ferner, daß doppelte Transposition etwas geringere Komplexität hat als Transposition mit doppelt so großer Breite[5], daß sie jedoch als weitaus schwieriger zu brechen gilt. Aber letzteres Urteil bezieht sich nur auf die Fälle, in denen Exhaustion nicht mehr durchführbar ist.

12.4.3 Schließlich fällt noch auf, daß für VIGENÈRE-Substitutionen Z und ld Z nur von N^d bzw. von $d \cdot \text{ld}\, N$ abhängt und somit (für $N=2^k$) beim Übergang zu binärer Codierung gleich bleibt: $(2^k)^d = 2^{k \cdot d}$. Dagegen geht für PERMUTE-Substitutionen (12.3.1) die Komplexität beim Übergang zu binärer Codierung drastisch zurück: Es ist $((2^k)!)^d > (2!)^{k \cdot d}$ für $k \geq 2$.

12.5 Die Exhaustionsmethode

Die kombinatorische Komplexität ist eben nur ein Maß für eine *ganz bestimmte* Entzifferungsmethode; eine sehr allgemeine Methode allerdings, die wir **Exhaustion** nennen wollen: Es werden *alle* Klartexte, die nach einem gewissen Verfahren zu einem vorgegebenen Geheimtext passen (alle ‚Varianten'), konstruiert und es wird die „richtige" Nachricht „ausgelesen" — in des Wortes ‚Lesen' wahrster Bedeutung. Bei dieser Methode ‚liest' man unter Umständen mehr als eine Nachricht heraus — dann weiß man aber auch, daß die Entzifferung nicht eindeutig ist. Wir werden darauf unter dem Stichwort Unizitätslänge zurückkommen. Liest man gar keine Nachricht heraus, so handelt es sich entweder um einen Chiffrierfehler oder es liegt gar nicht das vermutete Verfahren vor.

Das Verfahren ist natürlich praktisch nur durchführbar, wenn die Anzahl der durchzumusternden Varianten nicht riesengroß ist. Man geht dabei auch so vor, daß man für längere Nachrichten nicht jeden möglichen Klartext sogleich ausdruckt, sondern für jede Variante jeweils ein Stück, im Extremfall jeweils ein Zeichen.

---

[5] Es steht $Z = (n!)^2$ gegen $Z = (2n)! = (n!)^2 \cdot \binom{2n}{n} \asymp (n!)^2 \cdot 4^n / \sqrt{\pi \cdot (n + \frac{1}{4} + \frac{1}{32 \cdot n})}$.

H V Z D U V F K R Q G X Q N H O D O V L F K L Q E R Q Q D Q N D P L F K C
I W A E V W G L S R H Y R O I P E P W M G L M R F S R R E R O E Q M G L D
J X B F W X H M T S I Z S P J Q F Q X N H M N S G T S S F S P F R N H M E
K Y C G X Y I N U T J A T Q K R G R Y O I N O T H U T T G T Q G S O I N F
L Z D H Y Z J O V U K B U R L S H S Z P J O P U I V U U H U R H T P J O G
M A E I Z A K P W V L C V S M T I T A Q K P Q V J W V V I V S I U Q K P H
N B F J A B L Q X W M D W T N U J U B R L Q R W K X W W J W T J V R L Q I
O C G K B C M R Y X N E X U O V K V C S M R S X L Y X X K X U K W S M R J
P D H L C D N S Z Y O F Y V P W L W D T N S T Y M Z Y Y L Y V L X T N S K
Q E I M D E O T A Z P G Z W Q X M X E U O T U Z N A Z Z M Z W M Y U O T L
R F J N E F P U B A Q H A X R Y N Y F V P U V A O B A A N A X N Z V P U M
S G K O F G Q V C B R I B Y S Z O Z G W Q V W B P C B B O B Y O A W Q V N
T H L P G H R W D C S J C Z T A P A H X R W X C Q D C C P C Z P B X R W O
U I M Q H I S X E D T K D A U B Q B I Y S X Y D R E D D Q D A Q C Y S X P
V J N R I J T Y F E U L E B V C R C J Z T Y Z E S F E E R E B R D Z T Y Q
W K O S J K U Z G F V M F C W D S D K A U Z A F T G F F S F C S E A U Z R
X L P T K L V A H G W N G D X E T E L B V A B G U H G G T G D T F B V A S
Y M Q U L M W B I H X O H E Y F U F M C W B C H V I H H U H E U G C W B T
Z N R V M N X C J I Y P I F Z G V G N D X C D I W J I I V I F V H D X C U
A O S W N O Y D K J Z Q J G A H W H O E Y D E J X K J J W J G W I E Y D V
B P T X O P Z E L K A R K H B I X I P F Z E F K Y L K K X K H X J F Z E W
C Q U Y P Q A F M L B S L I C J Y J Q G A F G L Z M L L Y L I Y K G A F X
D R V Z Q R B G N M C T M J D K Z K R H B G H M A N M M Z M J Z L H B G Y
E S W A R S C H O N D U N K E L A L S I C H I N B O N N A N K A M I C H Z
F T X B S T D I P O E V O L F M B M T J D I J O C P O O B O L B N J D I A
G U Y C T U E J Q P F W P M G N C N U K E J K P D Q P P C P M C O K E J B

Tabelle 5. 26 Varianten einer CAESAR-Chiffrierung: H V Z D U V F K R Q ...

Wir illustrieren das Verfahren an zwei Beispielen von Verfahren, die jeweils etwa zwei Dutzend Varianten haben:

a) CAESAR-Addition mit Z_{26}: 26 Varianten (Tabelle 5)

b) Transposition mit Periode 4: 24 Varianten (Tabelle 6)

Exhaustiv geht man auch vor, wenn man eine nicht zu große Anzahl ‚wahrscheinlicher Schlüsselwörter' vorliegen hat oder zu kennen glaubt. In der Renaissance war das diesbezügliche Repertoire geeigneter ‚geflügelter Worte' – *OMNIA VINCIT AMOR, VIRTUTI OMNIA PARENT, IN PRINCIPIO ERAT VERBUM, SIC ERGO ELEMENTIS,* um nur einige zu nennen, die in der Literatur auftreten – doch recht beschränkt. Aber auch heute findet man bei Amateuren bis hinauf zu Staatsmännern eine Vorliebe für ‚programmatische' Schlüsselwörter.

S A E W S H R C N U O D K L N E L I A S H N C I O N B N N A A K I H M C W
A S E W H S R C U N O D L K N E I L A S N H C I N O B N A N A K H I M C N
A E S W H R S C U O N D L N K E I A L S N C H I N B O N A A N K H M I C N
E A S W R H S C O U N D N L K E A I L S C N H I B N O N A A N K M H I C Z
S E A W S R H C N O U D K L N E L A I S H C N I O B N N N A A K I M H C W
E S A W R S H C O N U D N K L E A L I S C H N I B O N N A N A K M I H C Z
S W E A S C R H N D O U K E N L L S A I H I C N O N B N N K A A I C M H W
W S E A C S R H D N O U E K N L S L A I I H C N N O B N K N A A C I M H A
W E S A C R S H D O N U E N K L S A L I I C H N N B O N K A N A C M I H A
E W S A R C S H O D N U N E K L A S L I C I H N B N O N A K N A M C I H Z
E S W A R S C H O N D U N K E L A L S I C H I N B O N N A N K A M I C H Z
S W A E S C H R N D U O K E L N L S I A H I N C O N N B N K A A I C H N W
W S A E C S H R D N U O E K L N S L I A I H N C N O N B K N A A C I H M A
W A S E C H S R U U N D E L K N S I L A I N H C N N D B K A N A C H I M A
A W S E H C S R U D N D L F K N I S L A N I H C N N O B A K M A H C I M N
S A W E S H C R N U D O K L E N L I S A H N I C O N N B N A K A I H C M W
A S W E H S C R U N D D L K E N I L S A N H I C N O N B A N K A H I C M N
A W E S H C R S U D O N L E N K I S A L N I C H N N B O A K A N H C M I N
W A E S C H R S D U O N E L N K S I A L T N C H N N B O K A A N C H M I A
W E A S C R H S D O U N E N L K S A I L I C N H N B N O K A A N C M H I A
E W A S R C H S D D U N N E L K A S I L O I N H A N N D A K A N M C H I Z
A E W S H R C S U D O N L N E K I A S L N C I H N B N O A A K N H M C I N
E A W S R H C S O U D N N L E K A I S L O N I H B N N O A A K N M H C I Z
S E W A S R C H N D D U K N E L L A S I H C I N O B N N N A K A I M C H W

Tabelle 6. 24 Varianten einer Transposition der Breite 4: S A E W S H R C N U ...

12.6 Unizitätslänge

Verfolgt man den segmentweisen Aufbau der verschiedenen möglichen Klartexte, so merkt man, daß von einer recht gut abgrenzbaren Stelle an die Entscheidung für *einen* Klartext deutlich zu fällen ist. Die Anzahl Zeichen bis zu dieser Stelle nennt man die empirische **Unizitätslänge** U des betreffenden Verfahrens. Es fällt auf, daß in beiden Beispielen, bei ungefähr gleicher Komplexität ($Z \approx 25$ bzw. $\mathrm{ld}\, Z \approx 4.64$) die Unizitätslänge ungefähr gleich (nämlich bei etwa 4 Zeichen) ist [6].

Auch für Verfahren mit sehr großem Z, wie etwa monoalphabetische Chiffrierungen ($Z = 26!$, $\mathrm{ld}\, Z = 88.38$) kann die Unizitätslänge von erfahrenen Kryptologen abgeschätzt werden: für Texte mit deutlich weniger Buchstaben

[6] Es gibt beispielsweise nur ganz wenige Vierbuchstabenwörter, die keine eindeutige Caesar-Entschlüsselung erlauben, im Deutschen etwa (Z_{26}) zydd: BAFF, POTT; qfzg: LAUB, TICK; qunq: EIBE, OLSO; himy: ABER, NORD, KLOA(KE), (ST)OPSE(L) ($Z_{25}!$); im Englischen (Z_{26}) mpqy: ADEN, KNOW; aliip: DOLLS, WHEEL; afccq: JOLLY, CHEER (nur verschiedene Buchstaben sind hier von Belang).

gelingt keine eindeutige Entschlüsselung. Im Falle der allgemeinen monoalphabetischen Chiffrierung liegt die Unizitätslänge nach solchen Erfahrungen bei einigen Dutzend (*Sacco* 1947), genauer zwischen 20 und 30:

> *"... the unicity point, at about 27 letters. ... With 30 letters there is always a unique solution to a cryptogram of this type and with 20 it is usually easy to find a number of solutions"* (*Shannon* 1945);

> *"Practically, every example of 25 or more characters representing monoalphabetic encipherment of a 'sensible message' in English can be readily solved"* (*Friedman* 1973).

Für die allgemeine polyalphabetische periodische Chiffrierung (PERMUTE-Substitutionen) mit der Periode d ist die Unizitätslänge proportional der Länge des Schlüssels (*Sacco* 1947).

Kontrollexperimente mit erheblich größerem Z ergeben das empirische Resultat (siehe auch 15.11):

> Die Unizitätslänge hängt (bei ein und der selben Sprache) lediglich von der kombinatorischen Komplexität Z des Verfahrens ab, und ist für nicht zu kleine Z proportional $\operatorname{ld} Z$.

Dieses quantitative Resultat war um 1935 anscheinend wenig bekannt,[7] möglicherweise hatte *Friedman* eine Ahnung. Es bedeutet, daß der ganze Einfluß der dem Text zugrundeliegenden Sprache sich nur in der Proportionalitätskonstante auswirken kann, und ist ein empirischer Angelpunkt zur Begründung der *Shannon*'schen Informationstheorie. Die theoretische Untermauerung verdankt man *Claude E. Shannon* (1945, freigegeben 1949).

Nehmen wir einmal für einfache Substitution *Friedman*s Wert $U = 25$ an, so gilt also, mit $\operatorname{ld} Z \approx 88.38$ empirisch (für nicht zu kleines Z)

$$(*) \qquad U \approx \tfrac{1}{3.5} \operatorname{ld} Z .$$

Tabelle 7 zeigt eine nach dieser Formel mittels Tabelle 3 für verschiedene Breiten n gerechnete Aufstellung.[8]

	$n = 1$	$n = 4$	$n = 16$	$n = 64$	$n = 256$
Allgemeine Substitution	**25**	$2.3 \cdot 10^6$	10^{24}	10^{93}	10^{365}
Lineare homogene Substitution	(1.02)	21	345	5 520	88 000
Addition	(1.34)	6	21	86	345
Transposition		(1.31)	13	85	480

Tabelle 7. Empirische Unizitätslänge U, extrapoliert nach $(*)$, aufgerundet ($N = 26$)

[7] Lediglich qualitative Erkenntnisse, wie „der Schlüssel sollte der Länge nach mit der Nachricht vergleichbar sein" (*Parker Hitt* 1914, vgl. 8.8.2) waren seit *Kasiski*, s. 17.3, bekannt.

[8] Die eingeklammerten Werte fallen dabei zu klein aus, um bedeutungsvoll zu sein. Die Formel hat folgenden informationstheoretischen Hintergrund: Von $4.7 = \operatorname{ld} 26$ [$bit/char$] entfallen 3.5 [$bit/char$] (74.5%) auf Redundanz und 1.2 [$bit/char$] (24.5%) auf Information. Mehr darüber im Anhang *Perfekte Sicherheit und praktische Sicherheit*.

Für Bigramm-Permutation ergibt sich $U \approx 1539$, für Trigramm-Permutation $U \approx 63\,570$, für Tetragramm-Permutation $U \approx 2\,266\,500$.

Für polyalphabetische Chiffrierung vervielfacht sich die empirische Unizitätslänge einer zugrundeliegenden monoalphabetischen Chiffrierung mit der Periodenlänge d. So ergibt Addition (VIGENÈRE-Verfahren)

$$\begin{array}{lll} \text{mit} & d = 10^2 & U \approx 134 \\ \text{mit} & d = 10^4 & U \approx 13\,400 \\ \text{mit} & d = 10^6 & U \approx 1\,340\,000 \end{array}$$

Falls eine Unizitätslänge existiert, so ist zu erwarten, daß auch durch andere geeignete Methoden als durch Exhaustion das Brechen einer Chiffrierung mit wachsender Länge des Chiffrats weniger unsicher und ab einer gewissen, in der Nähe der Unizitätslänge liegenden Länge des Chiffrats unproblematisch wird, sobald ein hinreichender Aufwand getrieben wird. Für ‚unbrechbare' Chiffrierungen (vgl. 8.8.4) existiert keine Unizitätslänge.

12.7 Praktische Durchführung der Exhaustion

Bei der praktischen Durchführung eines Exhaustionsverfahrens wird man die Länge der zu betrachtenden Stücke schrittweise vergrößern und jeweils „unmögliche" Varianten ausmerzen. Nach den in der Literatur verfügbaren Tabellen sind von den 676 Bigrammen rund die Hälfte „möglich", von den 17 576 Trigrammen sind etwa ein halbes Tausend „möglich". Das Verfahren ist leicht mechanisierbar und mit Rechenanlagen interaktiv durchführbar, wenn man mit nicht wesentlich mehr als zehntausenden von Varianten beginnt. Bei Bildschirm-Betrachtung kann man unschwer Fünfer- bis Achtergruppen „mit einem Blick" erfassen und mindestens zwei solche Gruppen pro Sekunde „auslesen", was eine Stundenleistung von zehntausend Anfangsvarianten ergibt. Später vermindern sich die zu betrachtenden Anzahlen ganz drastisch. Für das Beispiel von Tabelle 5 bzw. Tabelle 6 ist das in Abb. 82 bzw. Abb. 83 ersichtlich. Dabei haben wir, um Randeinflüsse zu diminimieren, mit der 6. Spalte begonnen.

Exhaustion ohne maschinelle Unterstützung wird unerträglich, wenn einige Zehntausend Fälle zu untersuchen sind (der Acht-Stunden-Tag hat 28 800 Sekunden!). Beachte, daß nach 12.3.4 und 12.2.4

bei VIGENÈRE (einer additiven polyalphabetischen Chiffrierung)

$Z = 17\,576$ für Periode 3, $Z = 456\,976$ für Periode 4;

bei Transposition (einer speziellen polygraphischen Chiffrierung)

$Z = 40\,320$ für Breite 8, $Z = 362\,880$ für Breite 9.

Dies zeigt, welche (beschränkte) Tragweite die Exhaustionsmethode wirklich hat. Für allgemeine monoalphabetische Chiffrierung und PLAYFAIR-Verfahren, mit Z von der Größenordnung 10^{25}, ist sie praktisch bereits

V	VF	VFK?					
W	WG	WGL	WGLS?				
X	XH	XHM?					
Y	YI	YIN?					
Z	ZJ	ZJO	ZJOV	ZJOVU?			
A	AK	AKP?					
B	BL	BLQ?					
C	CM	CMR?					
D	DN	DNS?					
E	EO	EOT	EOTA	EOTAZ?			
F	FP	FPU	FPUB	FPUBA?			
G	GQ	GQV?					
H	HR	HRW?					
I	IS	ISX	ISXE	ISXED?			
J	JT?						
K	KU	KUZ	KUZG?				
L	LV	LVA	LVAH	LVAHG?			
M	MW	MWB?					
N	NX	NXC?					
O	OY	OYD	OYDK?				
P	PZ	PZE	PZEL	PZELK	PZELKA	PZELKAR?	
Q	QA?						
R	RB	RBG	RBGN	RBGNM?			
S	SC	SCH	SCHO	SCHON	SCHOND	SCHONDU	SCHONDUN•
T	TD	TDI	TDIP	TDIPO	TDIPOE	TDIPOEV?	
U	UE	UEJ?					

Abb. 82. Exhaustion für 26 Varianten einer CAESAR-Chiffrierung

H	HR	HRC	HRCN?				
S	SR	SRC?					
R	RS	RSC	RSCU	RSCUO?			
H	HS	HSC	HSCO	HSCOU	HSCOUN	HSCOUND	HSCOUNDN?
R	RH	RHC?					
S	SH	SHC?					
C	CR	CRH?					
S	SR	SRH	SRHD?				
R	RS	RSH	RSHD	RSHDO	RSHDON	RSHDONU?	
C	CS?						
S	SC	SCH	SCHO	SCHON	SCHOND	SCHONDU	SCHONDUN•
C	CH	CHR	CHRN?				
S	SH	SHR	SHRD?				
H	HS	HSR?					
C	CS?						
H	HC	HCR?					
S	SC	SCR?					
C	CR	CRS?					
H	HR	HRS	HRSD?				
R	RH	RHS?					
C	CH	CHS	CHSD	CHSDD?			
R	RC	RCS?					
H	HC	HCS?					
R	RC	RCH	RCHN	RCHND?			

Abb. 83. Exhaustion für 24 Varianten einer Transposition der Breite 4

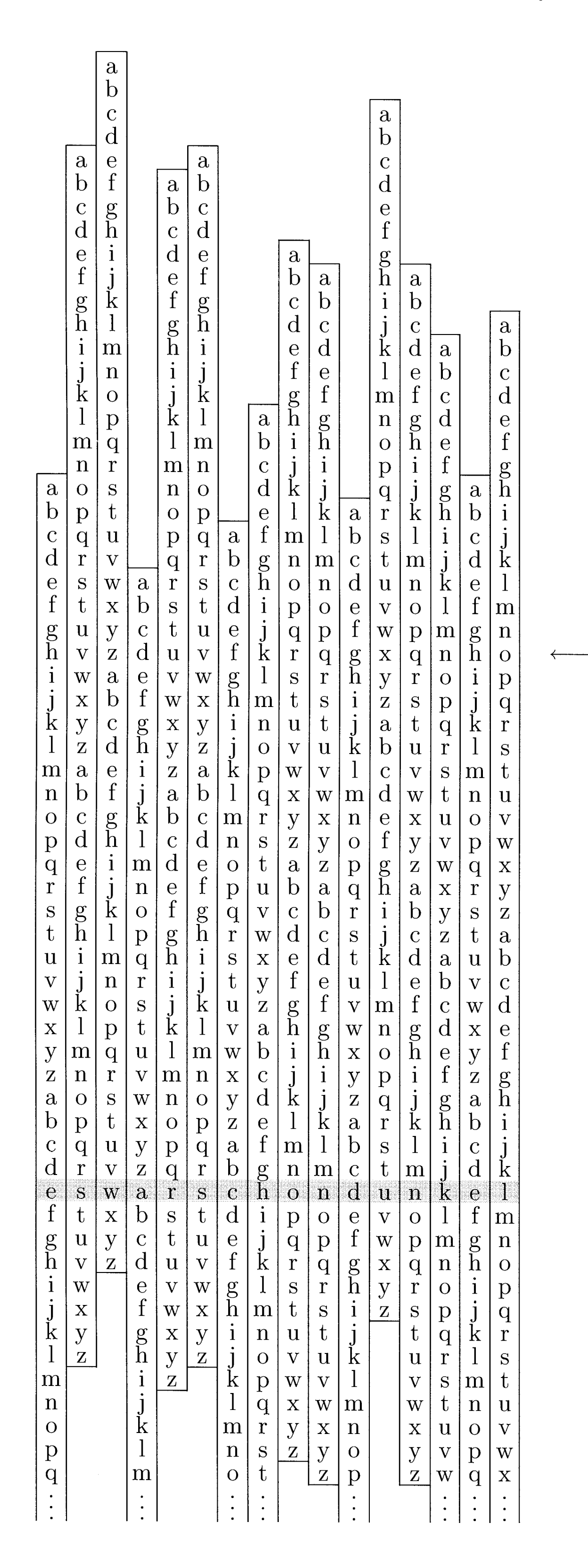


Abb. 84.
Steifenmethode für das Brechen einer CAESAR-Chiffrierung

nicht mehr verwendbar. Gegen die Exhaustionsmethode hilft jedoch eine noch so hoch erscheinende Komplexität nichts, wenn diese durch geeignete Maßnahmen hinreichend eingeengt werden kann.

Mit anderen Worten:

Die Exhaustionsmethode, obschon für sich allein ziemlich bedeutungslos, ist in Kombination mit anderen Verfahren die Grundmethode der Kryptanalyse.

Exhaustion wendet auch der berufene Entzifferer an bei polyphonen Chiffrierungen. Bekanntestes Beispiel ist die polyalphabetische Chiffrierung mit dem Zylinder von *Jefferson* und *Bazeries*, bei dem man den Klartext unter zwei Dutzend Varianten suchen muß.

12.8 Mechanisierung der Exhaustion

12.8.1 Für die Exhaustion einer CAESAR-Addition gibt es eine Mechanisierung durch die einfache **Streifenmethode**. Vorbereitete Streifen, auf denen das Alphabet (zweimal) verzeichnet ist, werden benutzt, um das Chiffrat und gleichzeitig alle Varianten darzulegen (Abb. 84). Statt dessen kann man auch Scheiben benutzen, auf deren Umfang das Alphabet steht.

12.8.2 Für die Exhaustion einer Transposition bekannter Breite n schreibt man das Chiffrat waagrecht laufend in ein Feld von n Spalten und zerschneidet dann das Blatt in n Streifen, die man permutiert (Abb. 85).

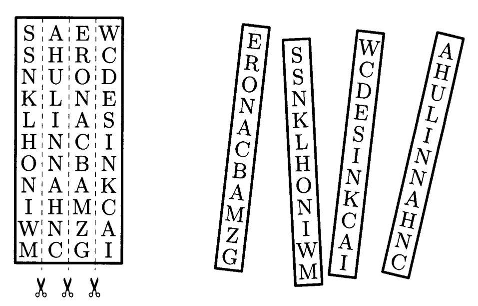


Abb. 85.
Schneidemethode
für das Brechen
einer Transposition

12.8.3 Kryptanalyse durch Exhaustion ist eine Methode der rohen Gewalt und hat als solche ihre Grenzen der Durchführbarkeit. In den nächsten Kapiteln werden wir Methoden diskutieren, die in raffinierter Weise auf Invarianten der Chiffrierung basieren ("the 'invariant' characteristics of the cryptographic system employed", Solomon Kullback, in: Statistical Methods in Cryptanalysis, 1935).

13 Anatomie der Sprache: Muster

"No matter how resistant the cryptogram, all that is really needed is an e n t r y, *the identification of* o n e *word, or of three or four letters."*

Helen Fouché Gaines 1939

Sprache enthält ein schwer ausrottbares inneres Gerüst von Gesetzmäßigkeiten. Von besonderer Wichtigkeit sind dabei Wiederholungsmuster.

13.1 Invarianz der Wiederholungsmuster

Invarianzsatz 1: Für alle monoalphabetischen, funktionalen einfachen Substitutionen , insbesondere auch für alle linearen monoalphabetischen einfachen Substitutionen gilt:
Wiederholungsmuster der Einzelzeichen innerhalb des Textes bleiben erhalten.

Wird etwa der Klartext	w i n t e r s e m e s t e r
durch einen CAESAR chiffriert	Z L Q W H U V H P H V W H U ,
mit einem revertierten Alphabet	D R M G V I H V N V H G V I ,
mit einem permutierten Alphabet	V A H O R M N R G R N O R M ,

so bleibt das Muster der Zeichenwiederholungen erhalten. Muster sind nach *Shannon* die *'residue classes'* der einfachen Substitutionen. Textstücke, die das gleiche Wiederholungsmuster aufweisen, heißen *idiomorph.*

Für monoalphabetische und funktionale *polygraphische* Substitutionen des Typs $V^{(n)} \longrightarrow W^{(m)}$ bleiben unter Beachtung der Polygrammfugen die Muster der Polygrammwiederholungen erhalten.

Transpositionen dagegen erhalten Wiederholungsmuster nicht. Auch homophone und ganz besonders polyalphabetische Substitutionen zerstören die Wiederholungsmuster.

Muster bezeichnet man üblicherweise in Normalform mit Ziffernfolgen, in denen jede erstmals auftretende Ziffer keine größere Ziffer zur Linken hat. N R G R N hat das Muster *12321* , N R G R N O R das Muster *1232142* , O R M N R G R N O R M das Muster *12342524123* .

Im Geheimtext V A H O R M N R G R N O R M
fällt das Muster *12321* von N R G R N sofort auf. Auch tritt das wiederholungsfreie Muster *123* von O R M zweimal auf. Das gesamte Muster *12345675857456* bedeutet also ein 6+8-buchstabiges Wort, das sich reimt. Tatsächlich wissen wir, wenn wir aufgepaßt haben, daß w i n t e r s e m e s t e r idiomorph ist, und können vermuten, daß es kaum eine andere Lösung gibt.

Kurze Muster erlauben jedoch viele Belegungen. Das Muster *1221* erlaubt im Englischen die in Abb. 86 zusammengestellten Belegungen. Die Liste (ohne Eigennamen) dürfte ziemlich vollständig die in *Cassels German Dictionary* aufgeführten Wörter (ohne grammatikalische Abarten) umfassen.

Beachte, daß diese Liste außer (b)atta(lion), (z)eppe(lin), (c)ommo(dore), (sh)ippi(ng) nur wenige Wörter aus dem militärischen Genre enthält; weiterhin außer (amb)assa(dor), assa(ssin), (sh)illi(ng), (perm)issi(ion) nur wenige Wörter aus dem diplomatischen Genre. Die Suche nach den Belegungen eines Musters wird durch die Kenntnis der Umstände erheblich eingeschränkt.

Neben *1221* sind andere interessante Vier-Ziffern-Muster aus zwei Ziffern *1211*, *1212*, *1121*, für die es Belegungen wie (p)fiff, gege(ben), (s)eele gibt, andere wie *1122* oder *1111* haben im Deutschen aus orthographischen Gründen keine natürlichen Belegungen. Beachte auch, daß ein Muster wie *12324 5678* verlangt, daß die acht beteiligten Zeichen verschieden sind; andernfalls sollte das Muster vielleicht *∗232∗∗∗∗∗* lauten und wäre nicht verschieden von *121*. Ein nicht zu langes Muster mit zwei oder mehr wiederholten Ziffern hat normalerweise, wenn überhaupt, sehr wenige Belegungen oder eine eindeutige. *12132435* erlaubt im Englischen nur /fiftieth/.

Die Schlußfolgerung ist klar: Wörter und Phrasen mit einem auffälligen Muster sollten durch den Kryptosekretär eliminiert werden, normalerweise durch Umschreibung, wie es regelmäßig für den Funkverkehr der britischen Admiralität geschah. Ein notorisches Beispiel ist *1234135426*, das im Deutschen nichts als das ominöse /heilhitler/ erlaubt. Wer hätte es in Hitlers Deutschland wagen dürfen, die stereotype Floskel zu entfernen? *Kerckhoffs* hat sogar darauf hingewiesen, daß Wiederholungen wie in ≪*pouvez-vous vous défendre*≫ zu vermeiden seien. Aber in klarem Gegensatz dazu war es im militärischen Verkehr weithin üblich, eine wichtige Stelle durch Wiederholung hervorzuheben, wie `OKMMMANAN` (vgl. 9.2.5) in deutschen Funksprüchen. Die Alliierten taten das gleiche: `SC48SC48` findet sich in einem Funkspruch an den Konvoi SC.48 (*Beesly*) oder `CHICKEN-WIRE£CHICKEN-WIRE` in einer Nachricht, mit der *Bletchley Park* die Entzifferung eines deutschen Funkspruchs, der amerikanische Paßwörter und Antworten enthielt, weitergab (*Lewin*).

Die Anzahl von Mustern der Länge n stimmt überein mit der Anzahl von Partitionen einer n-elementigen Menge, den **Bell-Zahlen** $B(n)$, die mit n ziemlich rasch wachsen, wie die folgende Tabelle zeigt:

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$B(n)$	1	1	2	5	15	52	203	877	4 140	21 147	115 975	678 570	4 213 597

abbacy cabbage cabbala sabbath scabbard baccalaureate maccabee staccato affable affair baggage braggart haggard laggard allah allay ballad ballast fallacy gallant installation mallard palladium parallax wallaby diagrammatic flammable gamma grammar mamma programmatic annalist annals bandanna cannabis hosanna manna savannah appal apparatus apparel apparent kappa arrack arraign arrange arrant arras array barrack barracuda barrage carragheen embarrass narrate tarragon warrant ambassador assail assassin assault assay cassandra massacre massage passage vassal wassail attach attack attain rattan attar battalion coattail rattan regatta wattage piazza beebread boob booby deed deedless indeed doodle ebbed eccentric bedded reddear redden shredder wedded effect effeminate effendi efferent effervesce effete begged bootlegger egged legged pegged trekked aquarelle bagatelle belle chancellery chanterelle driveller dweller excellent feller fontanelle gazelle groveller hellebor hellenic impellent intellect jeweller libeller mademoiselle nacelle pellet propeller repellent seller teller traveller emmet barrenness comedienne fennec fennel jennet kennel rennet tenner pepper stepper zeppelin deterrent ferret interregnum interrelation overreact parterre terrestrial adressee dessert dresser essence essential finesse largesse lessen messenger noblesse quintessence tesselate vessel begetter better burette corvette curette fetter gazette getter letter marionette pirouette rosette roulette setter silhouette geegee googol heehaw capriccio pasticcio forbidding yiddish difficile difficult griffin tiffin biggish bacilli billiard billion brilliant chilli cyrillic fillip illicit illinois illiquid illiberal illiterate illimitable lilliput milliard millibar milligram milliliter millimeter milliner millionaire millivolt penicillin postillion shilling silliness tranquillize trillion trillium vanillin gimmick immigrant imminent immiscible immitigable finnish innings pinniped zinnia pippin irrigate irritate admission commission dissident dissimilar dissipate emission fissile fission fortissimo missile mission missive omission permission permissive acquitting fitting kittiwake civvies noon broccoli sirocco apollo collocate colloid colloquial colloquium follow hollow rollout common accommodate commode commodore commotion connote opponent opportune oppose opposite borrow corroborate corrode horror morrow sorrow blossom crossover blotto bottom cotton grotto lotto motto ottoman risotto glowworm powwow peep poop career seesaw teeter teethe teetotal teetotum toot toothache tootle hubbub succulent succumb succuss pullup nummulite unnumbered chaussure guttural

Abb. 86. Belegungen des Musters *1221* im Englischen
(nach *Hugh Casement*)

13.2 Ausschließung von Chiffrierverfahren

Satz 1 kann negativ zur Ausschließung von monoalphabetischen, funktionalen einfachen Substitutionen gebraucht werden – wenn nämlich Muster vorkommen, für die es keine Belegung gibt. Jedoch ist Vorsicht geboten: Speziell das Fehlen von Zeichenverdopplungen besagt nicht viel. Seit *G. B.* und *M. Argenti* gilt es für professionelle Kryptographen als selbstverständlich, zur Abwehr der Mustersuche bereits im Klartext Zeichenwiederholungen zu unterdrücken, also etwa *sigilo* statt *sigillo* zu benutzen (vgl. 11.1.5). Auch die klassische Unterdrückung des Wortzwischenraums soll die Musterbildung vermindern. Unterdrückung von Zeichen kann zu Polyphonie führen. Daß durch Unterdrückung des Wortzwischenraums Wörter „zusammenfließen“, ist selten, kann aber vorkommen: „er soll ab erhalt kommen“ – „er soll aber halt kommen“, oder ‘we came to get her’ – ‘we came together’.

13.3 Mustersuche

Satz 1 kann positiv benutzt werden, wenn man Grund hat zu der Annahme, daß eine monoalphabetische, funktionale einfache Substitution vorliegt. Beispiele solcher Art finden sich in Lehrbüchern, die für den Amateur bestimmt sind, häufig.

13.3.1 Im folgenden Beispiel von *Helen Fouché Gaines* (␣ bezeichnet nicht unterdrückte Zwischenräume) mit vermuteter einfacher Substitution

F D R J N U ␣ H V X X U ␣ R D ␣ M D ␣ S K V S O ␣ P J R K ␣ Z D
Y F Z J X ␣ G S R R V T ␣ Q Y R ␣ WD A R WD F V ␣ R K V ␣ D R
K V T ␣ D F ␣ S Z Z D Y F R ␣ D N ␣ N V O V T S X ␣ S A WV Z R

ist nach Meinung der Autorin das Auftreten von D in jedem der vier zweibuchstabigen Wörter auffällig. Dies legt den Einstieg D ≙ o nahe. Ferner könnte RKV ≙ the gelten, was verträglich wäre mit RD ≙ to und DRKVT ≙ other ; und GSRRVT ≙ GStter ergäbe. Jetzt hat man bereits folgendes Fragment einer Entzifferung mit vermutlich fünf erkannten Zeichen

F o t J N U ␣ H e X X U ␣ t o ␣ M o ␣ S h e S O ␣ P J t h ␣ Z o
Y F Z J X ␣ G S t t e r ␣ Q Y t ␣ Wo A t Wo F e ␣ t h e ␣ o t
h e r ␣ o F ␣ S Z Z o Y F t ␣ o N ␣ N e O e r S X ␣ S A We Z t

Von jetzt an geht es schneller: Für das andere Dreibuchstabenwort QYt scheiden not , got , out , yet aus, da e und o schon bestimmt sind, aber but wäre geeignet. Des weiteren könnten oF ≙ on und oN ≙ of (oder umgekehrt) passen. Im ersteren (glücklichen) Fall hat man bereits folgendes Fragment einer Entzifferung mit vermutlich neun erkannten Zeichen

n o t J f U ␣ H e X X U ␣ t o ␣ M o ␣ S h e S O ␣ P J t h ␣ Z o
u n Z J X ␣ G S t t e r ␣ b u t ␣ Wo A t Wo n e ␣ t h e ␣ o t
h e r ␣ o n ␣ S Z Z o u n t ␣ o f ␣ f e O e r S X ␣ S A We Z t

Das läßt sich schon sehen; SZZount liest sich als account und damit findet man auch ZounZJX , nämlich councJX als council . Somit hat man bereits folgendes Fragment

n o t i f U␣H e l l U␣t o␣Mo␣a h e a O␣P i t h␣c o
u n c i l␣G a t t e r␣b u t␣Wo A t Wo n e␣t h e␣o t
h e r␣o n␣a c c o u n t␣o f␣f e O e r a l␣S A We c t

das man mühelos ergänzt, bis auf Helly , was womöglich ein Eigenname ist.

Die hier gezeigten Phasen der Entzifferung können als „Trab“ (wenn nach dem Einstieg drei bis fünf Zeichen gefunden sind) und „Galopp“ (wenn acht bis zwölf Zeichen gefunden sind) bezeichnet werden. Dies spiegelt sich im Aufbau der Dechiffriertabelle wider:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
			o							h							t		r		e				
					n								f			b								u	
									i									a					l		c
s						m						g		d	w					y		p			

Lediglich H fehlt noch, B, C, E, I, L kommen im Geheimtext nicht vor.

An dieser Stelle sollte man sich erinnern, daß N und F sich gegenseitig ersetzten, (DF, DN) wurden zu (oN, oF). Das gleiche ist anscheinend für A und S, D und O, P und W, R und T, U und Y der Fall. Sollte eine echt involutorische Chiffrierung vorliegen, so ergäbe sich zu K $\hat{=}$ h symmetrisch H $\hat{=}$ k , Helly wäre als kelly zu lesen. Die ganze Chiffrierung würde lauten

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
s	q	z	o	v	n	m	k	j	i	h	x	g	f	d	w	b	t	a	r	y	e	p	l	u	c

Da die unterstrichenen Buchstaben der unteren Reihe rückwärts laufen, liegt vermutlich eine Konstruktion des Substitutionsalphabets mittels eines memorierbaren Kennwortes vor. In der Tat ergibt sich durch Umordnen die involutorische Substitution[1]

	c	u	l	p	e	r	a	b	d	f	g	h	i
↕	z	y	x	w	v	t	s	q	o	n	m	k	j

.

Der Staatsanwalt könnte auf diese völlig plausible Entzifferung unter vollständiger Bloßlegung des Systems eine Anklage bauen. **Rohrbachs Forderung** lautet: „Erst mit der Erarbeitung sämtlicher zugehörigen Schlüssel wird die Lösung als beendet angesehen“ (*Hans Rohrbach* 1946). Dies ist wichtig, wenn Kryptanalysten wie *Bazeries* 1898 im Prozeß gegen den Herzog von Orléans oder *Elizebeth Friedman*, die Ehefrau von *W. F. Friedman*, 1933 im Prozeß gegen die Consolidated Exporters Company, eine Schmuggelorganisation zur Zeit der Prohibition, als Zeugen vor Gericht aussagen.

---

[1] *Samuel Woodhull* und *Robert Townsend* belieferten 1779 General *Washington* mit wertvollen Informationen aus dem von englischen Truppen besetzten New York. Sie benutzten als Decknamen CULPER SR. und CULPER JR., vgl. 4.4.1. Die angelsächsische (amerikanische) kryptologische Literatur benutzt *CULPER* häufig, um Schlüssel zu konstruieren. Im vorliegenden Beispiel ist die Substitution allerdings (Gaines, S. 70) mit dem Kennwort *CULPEPER* gebildet worden (vgl. 3.2.5). *Edmund Culpeper*, 1660-1738, war ein berühmter englischer Instrumentenmacher.

Cryptoquip

K I O S P X F I E V B O S F E F P M H Y I M K K J X F I E V B J F K Y F I - K O M H

Yesterday's Cryptoquip— GLUM GOLFER TODAY STUDIES SNOWMEN ON FAIRWAY.

Today's Cryptoquip clue: S equals C

The Cryptoquip is a simple substitution cypher in which each letter used stands for another. If you think that X equals O, it will equal O throughout the puzzle. Single letters, short words, and words using an apostrophe can give you clues to locating vowels. Solution is accomplished by trial and error.

Cryptoquip

K R K K R L H P L R U I O Z G K A Y M- M G O R A U L Y P Q , Q R U A H U L Z I U

Yesterday's Cryptoquip— TRICK HARMONICA MAKES PRETTY HARMONY AT PARTIES.

Today's Cryptoquip clue: I equals M

The Cryptoquip is a simple substitution cypher in which each letter used stands for another. If you think that X equals O, it will equal O throughout the puzzle. Single letters, short words, and words using an apostrophe can give you clues to locating vowels. Solution is accomplished by trial and error.

Abb. 87. Cryptoquips aus Los Angeles Times, 1977

13.3.2 Es sollte klar sein, daß die Entzifferung des obigen Beispiels nur deshalb so glatt lief, weil die Wortzwischenräume – im Gegensatz zu den professionellen Gepflogenheiten – nicht unterdrückt waren. Dies ist aber gerade die Spielregel für die in amerikanischen Zeitschriften häufig zu findenden 'Cryptos' (Abb. 87), zumindest für die Sorte, die als 'aristocrats' läuft: Wortzwischenräume und Interpunktionen bleiben streng erhalten; nur Buchstaben sind als Geheimtext-Alphabet erlaubt. Kein Buchstabe darf für sich selbst stehen. Die Länge ist bei den echten Aristokraten (ohne 'clues') 75 bis 100 Zeichen, also ziemlich lang in Anbetracht der Unizitätslänge $\approx$25 einer einfachen Substitution mit permutiertem Alphabet; dafür darf der Text aber die ausgefallensten amerikanischen Wörter enthalten (jedoch keine Fremdwörter) und braucht, außer grammatikalisch korrekt zu sein, keinen tieferen Sinn zu haben; kann also u.U. ebenso schwer zu „verstehen" sein wie das Kryptogramm. Wörter aus der Biologie wie *pterodactyl* und *ichtyomancy* können ebenso vorkommen wie das den Mathematikern vorbehaltene *syzygy*; aber auch *yclept*, *crwth* und *cwm* kann sich finden. Der Text kann so gewählt sein, daß die normalen Häufigkeiten der Buchstaben und Phrasen vollkommen verfälscht sind – daß also die in Kapitel 15 zu besprechenden, auf Häufigkeitsanalysen beruhenden Methoden gar nichts nützen ('the encipherer's full attention has been given to manipulation of letter characteristics', Helen Fouché-Gaines).

Bei *Kahn* findet sich die Lösung eines Kryptogramms der Sorte Aristokrat, das sich selbst beschreibt:

> *Tough cryptos contain traps snaring unwary solvers: abnormal frequencies, consonantal combinations unthinkable, terminals freakish, quaint twisters like ‚myrrh'.*

13.3.3 Es gibt beispielsweise Texte (**Lipogramme**), die gänzlich ohne /e/ geschrieben sind; der berühmteste ist der (literarisch eher anspruchslose) Ro-

man 'Gadsby' von *Ernest Vincent Wright* (Wetzel Publishing Co., Los Angeles 1939, 287 S., siehe Abb. 88). Auf dieser Masche, aber mit höheren Ansprüchen, ritt auch *Georges Perec* (1936–1982) mit seinem Roman *'La disparation'* (1969; deutsche Übers. 'Anton Foyls Fortgang' von *Eugen Helmlé*, Frankfurt a. M. 1986; engl. Übers. *A Void* von *Gilbert Adair*, 1995). *Perec*, der sich auch mit Akronymen und Akrostichons, Anagrammen und Palindromen spielerisch umgibt und der wie *Otto Promber*, *Oskar Pastior* und *Herbert Pfeiffer* einem Sprachaktionismus huldigt – er setzt auch Computerprogramme ein und legte 1969 ein Palindrom von 5 000 Buchstaben vor – hat 1973 die Geschichte der Lipogramme etwas aufgehellt; schon 1820 erschien in Wien der Roman eines *Dr. Franz Rittler* „Die Zwillinge", der ganz ohne /r/ geschrieben ist. Aber bereits um 1800 schrieb *Gavrila Romanovich Dershavin*, ein bedeutender russischer Dichter (1743–1816), den Roman „Ein Scherzwunsch", der ganz ohne /r/ und mit wenigen /o/ auskommt.

XXIX

GADSBY WAS WALKING back from a visit down in Branton Hills' manufacturing district on a Saturday night. A busy day's traffic had had its noisy run; and with not many folks in sight, His Honor got along without having to stop to grasp a hand, or talk; for a Mayor out of City Hall is a shining mark for any politician. And so, coming to Broadway, a booming bass drum and sounds of singing, told of a small Salvation Army unit carrying on amidst Broadway's night shopping crowds. Gadsby, walking toward that group, saw a young girl, back towards him, just finishing a long, soulful oration, saying:—

". . .and I can say this to you, for I know what I am talking about; for I was brought up *in a pool of liquor!!"*

As that army group was starting to march on, with this girl turning towards Gadsby, His Honor had to gasp, astonishingly:—

"Why! Mary Antor!!"

"Oh! If it isn't Mayor Gadsby! I don't run across you much, now-a-days. How is Lady Gadsby holding up during this awful war?"

[201]

Abb. 88. Seite aus 'Gadsby' von *Ernest Vincent Wright*

Wright schrieb im Vorwort, daß er die Type /e/ auf seiner Schreibmaschine totgelegt hatte, weil ihm manchmal zwanghaft ein /e/ in den Text schlüpfen wollte. Kryptologisch haben diese Monstrositäten natürlich ebenso wenig Belang wie die kryptologischen Verzierungen, die *Vladimir Nabokov* in seine

literarischen Werke einfließen ließ. *Vaclav Havel* hingegen machte sich über die marxistisch-leninistische Partei-(Geheim-)Sprache, das *Ptydepe*, und ihren bürokratischen Nachfolger, das *Chorukor*, lustig.

Auch Texte wie die letzten Worte in 'Finnegans wake' von *James Joyce*: *'End here. Us then. Finn, again! Take. Bussoftlee, mememormee! Till thousendsthee. Lps. The keys to. Given! A way a lone a last a loved a long the.'* bereiten einem Entzifferer große Mühe. Nicht umsonst enthält *James Joyce*s 'Ulysses' kryptologische Elemente.

13.4 Mustersuche bei polygraphischer Chiffrierung

Auffällige Muster zu unterdrücken, ist unter anderem die Absicht bei Verwendung eines Codes.

13.4.1 Durch mangelnde Sorgfalt bleiben sie trotzdem erhalten. *Luigi Sacco*, 1918 Leiter des '*Reparto crittografico*' des italienischen Hauptquartiers an der Isonzo- und Piave-Front, später Autor eines berühmten Buches, empfing am 30. Juni 1918 zwei Funksprüche (in Fünfergruppen) mit dem gleichen Ende

. . . . 4 92073 06583 47295 89255 07325 58347 29264 .

War schon das ein grober Schnitzer der Österreicher, so war noch schlimmer, daß sich der Teiltext 073**5834729 in kurzem Abstand von 18 Zeichen wiederholte. Dies war ein klarer Hinweis auf einen Code aus Dreiergruppen

... ... 492 073 065 834 729 589 255 073 255 834 729 264

Sacco hatte einige Erfahrung mit österreichischen Gewohnheiten und Grund zu der Vermutung, daß fahrlässigerweise ein längeres Wort buchstabenweise codiert worden war. Das Muster war *123456727458* und *Sacco*, ein Ingenieur, hatte den glänzenden Einfall, r a d i o s t a t i o n herauszulesen. Der faule österreichische Chiffrierer hatte es nicht für nötig gehalten, die Codegruppen für r a d i o und s t a t i o n aufzusuchen. Wenn aber schon einmal – für Eigennamen etwa – buchstabenweise codiert werden mußte, dann durfte eine solche Preisgabe des Codes für Einzelbuchstaben nicht am Anfang oder am Ende des Textes geschehen. Jedenfalls, der Einstieg in die Entzifferung anderer buchstabenweise codierter Textstellen und damit zum Brechen des ganzen Codes war geschafft.

13.4.2 Aber auch ohne die Phantasie *Sacco*s erlaubt das Beispiel einen Einstieg, wenn man eine Liste aller Muster und ihrer Belegungen verfügbar hat. Im vorliegenden Fall eines Musters der Länge 12, das vier Wiederholungen aufweist, findet man darin höchstwahrscheinlich kaum eine andere Belegung als r a d i o s t a t i o n , und wenn schon, gibt ein Durchspielen einiger weniger Fälle sofort Aufschluß.

Ohne Zweifel waren auch die Österreicher kryptanalytisch versiert. In der *Kriegschiffrengruppe* unter Oberst *Ronge* gab es eine italienische Sektion, in der Major (später Oberst) *Andreas Figl* ausgezeichnete Arbeit leistete, wie auch sein Kollege *Herrmann Pokorny* in der russischen Sektion – großzügig unterstützt durch die Stupidität der jeweiligen gegnerischen Dienste.

13.5 Die Methode des wahrscheinlichen Wortes

Bisher wurde nicht mehr vorausgesetzt als eine Vermutung über die natürliche Sprache des Klartextes. Nun wird auch andere Information herangezogen. Zum Einstieg in das Brechen einer monoalphabetischen einfachen Substitution dient insbesondere die Methode des „wahrscheinlichen Wortes" (frz. *mot probable*, engl. *probable word, crib*[2]), vgl. 11.2.5. Nunmehr sucht man nicht im Chiffrat nach einem auffälligen Muster, sondern man wählt ein Wort aus, das „wahrscheinlich" im Klartext vorkommt, und sucht das Chiffrat ab, ob es und wenn ja, wo überall es das *Muster* dieses Wortes enthält.

13.5.1 Dieses Vorgehen beschrieb schon *Giovanni Battista Porta* (1535-1615) in *De furtivis*, 1563. Statt eines Wortes verwendet man gerne auch eine ganze Phrase, wie „Oberkommando der Wehrmacht"; vor allem eignen sich dazu die am Anfang und am Schluß von Klartexten häufig zu findenden stereotypen Wendungen wie *reference to your letter*, *Hochachtungsvoll Ihr* – falls sie nicht von einem geschulten Chiffrierer entfernt wurden. Beispiele wie

An SS-Gruppenführer Generalleutnant der Waffen-SS Berger, Berlin W.35, SS-Hauptamt, mit der Bitte um absprachegemässe Weitergabe

From Algeria to Washington, 21. 7. To the State Department in Washington. Strictly confidential. Most urgent and personal for Deputy Under State Secretary. From Murphy

zeigen, daß es an *cribs* gewöhnlich nicht fehlt.[3] Im übrigen hilft Grips, Einblick und Einfühlungsvermögen in die gegnerische Situation, eine Kettenreaktion, die *Jack Good* mit *"success leading to more success"* treffend beschrieb. Und wenn keine Anhaltspunkte vorliegen, können welche provoziert werden: Im Gefolge kriegerischer Handlungen sind Wörter wie Angriff/*attack* und Granatfeuer/*shellfire*, Bombardierung/*bombardement* und Gefangener/*prisonnier* zu erwarten. Ist etwa den Umständen nach *division* ein „wahrscheinliches Wort" und eine Suche nach dem Muster *12131* von (d)ivisi(on) angebracht, so zeigt ein Blick auf Abb. 95 zeigt, daß im militärischen Genre die Gefahr, ein falsches Wort mit diesem Muster zu finden, gar nicht so groß ist, wie man angesichts seiner Kürze vermuten möchte.

13.5.2 Unsterbliche Verdienste für einen durchschlagenden Erfolg der Deutschen im 2. Weltkrieg erwarb sich 1941 der amerikanische Diplomat und spätere stellvertretende Unterstaatssekretär im Außenministerium *Robert D. Murphy* (1894-1978), der darauf bestand, seiner Bedeutung entsprechend in seinen Telegrammen stets *"From Murphy"* oder *"For Murphy"* zu verwenden (vgl. 11.1.3). Den Vogel schoß jedoch ab der ebenfalls in 4.4 erwähnte Leutnant *Jäger*. Disziplin ist etwas anderes als Gehorsam, sie erfordert Köpfchen, und damit hapert es überall.

---

[2] Im englischen Slang *crack a crib*, in ein Haus einbrechen.

[3] Selbst die „russische Kopulation" (vgl. 11.1.1) eines Klartextes – das willkürliche Zerschneiden und Zusammensetzen verkehrt herum – reicht nicht aus; auffällige Muster und Wiederholungen ganzer Wörter müssen vollständig entfernt werden.

13.5.3 Wie viel ein einziges wahrscheinliches Wort bringen kann, zeigt folgendes, von *U. Kratzer* stammendes fiktives Beispiel (Abb. 89), dem als Klartext ein berüchtigter „Führerbefehl“ von 1939 zugrundeliegt. Nach den Umständen wäre denkbar, daß das Jahr 1939 im Klartext vorkommt, und angesichts des Schwulsts, mit dem Hitlers Generäle dessen Verlautbarungen ausstatteten, wäre nicht einmal auszuschließen, daß, entgegen aller Vorsicht, „**neun**zehnhundert**neun**unddreissig“ ausgeschrieben vorkäme. Das würde die Suche nach dem Muster *1231* von **neun** nahelegen, obschon es sehr kurz ist und zahlreiche Fehltreffer zu befürchten wären.

Tatsächlich kommt dieses Muster etliche Male vor (Abb. 90), insbesondere als **HQGH** viermal, als **QHXQ** zweimal in der drittletzten und einmal in der vorletzten Zeile. Dabei hat das letzte Vorkommnis in der drittletzten Zeile vom Vorkommnis in der vorletzten Zeile gerade den richtigen Abstand für „**neun**zehnhundert**neun**“. Dieser durch die Wiederholung von **QHXQ** provozierte Einstieg liefert die fragmentarische Entzifferung von Abb. 91.

Offensichtlich befinden sich am Ende des Textes Datumangaben. Es drängt sich auf, den Schluß als „**vi**e**r**uh**r**f**ue**nf**u**n**d**vi**e**r**zig**“ zu lesen. Damit sind bereits 12 Zeichen entziffert:

. . . d e f g h i . . . . n . . . r . t u v . . . z
. . . G H I J K L . . . . Q . . . U . W X Y . . . C

und es ergibt sich die fragmentarische Entzifferung von Abb. 92. Darin kommt nun ganz zwingend mit **gehei**P**e** in Zeile 1 m≙P, mit **deut**VF**h** in Zeile 5 s≙V und c≙F, mit **getr**R**ffenen** in Zeile 10 o≙R, mit D**ngriff** in Zeile 15/16 a≙D. Es sind also jetzt schon 17 Zeichen wiederhergestellt:

a . c d e f g h i . . . m n o . . r s t u v . . . z
D . F G H I J K L . . . P Q R . . U V W X Y . . . C

Abb. 93 zeigt das zugehörige Zwischenergebnis, das sich schon recht flüssig liest und Abb. 94 das Endergebnis, die „Weisung Nr. 1 für die Kriegsführung“.

Spätestens jetzt stellt sich übrigens heraus, daß die Chiffrierung durch eine CAESAR-Addition erfolgte. Hätte man nur zu Anfang eine diesbezügliche Exhaustion versucht, hätte man dies natürlich nach wenigen Schritten bemerkt.

Das Beispiel ist selbstverständlich fiktiv; ein Anweisung dieser Brisanz geht regulär nicht über Funk, sondern durch Kurier und bräuchte damit überhaupt nicht chiffriert zu werden – schon gar nicht mit einem CAESAR! Wer genügend Phantasie hat, mag sich aber vorstellen, der dem Widerstand verbundene *Canaris* habe den Text weitergegeben und ein einfacher Agent habe ihn nach Schweden gefunkt.

13.5.4 Das Beispiel wäre jedoch genauso verlaufen, wenn irgend eine andere monoalphabetische Substitution zugrunde gelegen hätte. Es zeigt damit, daß die Mustererkennungsmethode von der Art der einfachen Substitution, gegen die sie gerichtet ist, gänzlich unabhängig ist.

J H K H L P H N R P P D Q G R V D F K H Z H L V X Q J Q U H
L Q V I X H U G L H N U L H J V I X H K U X Q J Q D F K G H
P D O O H S R O L W L V F K H Q P R H J O L F K N H L W H Q
H U V F K R H S I W V L Q G X P D X I I U L H G O L F K H P
Z H J H H L Q H I X H U G H X W V F K O D Q G X Q H U W U D
H J O L F K H O D J H D Q V H L Q H U R V W J U H Q C H C X
E H V H L W L J H Q K D E H L F K P L F K C X U J H Z D O W
V D P H Q O R H V X Q J H Q W V F K O R V V H Q G H U D Q J
U L I I D X I S R O H Q L V W Q D F K G H Q I X H U G H Q I
D O O Z H L V V J H W U R I I H Q H Q Y R U E H U H L W X Q
J H Q C X I X H K U H Q P L W G H Q D E D H Q G H U X Q J H
Q G L H V L F K E H L P K H H U G X U F K G H Q L Q C Z L V
F K H Q I D V W Y R O O H Q G H W H Q D X I P D U V F K H U
J H E H Q D X I J D E H Q Y H U W H L O X Q J X Q G R S H U
D W L R Q V C L H O E O H L E H Q X Q Y H U D H Q G H U W D
Q J U L I I V W D J H U V W H U Q H X Q W H U Q H X Q C H K
Q K X Q G H U W Q H X Q X Q G G U H L C L J D Q J U L I I V
C H L W Y L H U X K U I X H Q I X Q G Y L H U C L J

Abb. 89. Fiktives Chiffrat eines „Führerbefehls“ aus dem Jahr 1939

J H K **H L P H** N R P P D Q G R V D F K H Z H L V X Q J Q U H
L Q V I X H U G L H N U L H J V I X H K U X Q J Q D F K G H
P D O O H S R O L W L V F K H Q P R H J O L F K N **H L W H** Q
H U V F K R H S I W V L Q G **X P D X** I I U L H G O L F K **H P**
Z H J H **H L Q H I X H U G H** X W V F K O D **Q G X Q** H U W U D
H J O L F K H O **D J H D** Q V **H L Q H** U R V W J U **H Q C H** C X
E H V H L W L J H Q K D E H L F K P L F K C X U J H Z D O W
V D P H Q O R H V X **Q J H Q** W V F K O R V V **H Q G H** U D Q J
U L I **I D X I** S R O H Q L V W Q D F K G H Q I X **H U G H** Q I
D O O Z H L V V J H W U R I I H Q H Q Y R **U E H U** H L W X **Q**
J H Q C X I X **H K U H** Q P L W G H Q D E D **H Q G H** U X Q J H
Q G **L H V L** F K E H L P K H H **U G X U** F K G H Q L Q C Z L V
F K H Q I D V W Y R O O **H Q G H** W H Q D X I P D U V F K **H U**
J H E H Q D X I J D E **H Q Y H U W H** L O X **Q J X Q** G R S H U
D W L R Q V C L H O E O **H L E H** Q X Q Y **H U D H Q G H** U W D
Q J U L I I V W D J H U V W H U **Q H X Q** W H U **Q H X Q** C H K
Q K X Q G H U W **Q H X Q** X Q G G U H L C L J D Q J U L I I V
C H L W Y L H U X K U I X H Q I X Q G Y L H U C L J

Abb. 90. Vorkommen des Musters *1231*.
Das fettgedruckte Idiomorph QHXQ tritt dreimal, HQGH tritt viermal auf

J e h e L P e N R P P D n d R V D F h e Z e L V u n J n r e
L n V I u e r d L e N r L e J V I u e h r u n J n D F h d e
P D O O e S R O L t L V F h e n P R e J O L F h N e L t e n
e r V F h R e S I t V L Q d u P D u I I r L e d O L F h e P
Z e J e e L n e I u e r d e u t V F h O D n d u n e r t r D
e J O L F h e O D J e D n V e L n e r R V t J r e n z e z u
E e V e L t L J e n h D E e L F h P L F h z u r J e Z D O t
V D P e n O R e V u n J e n t V F h O R V V e n d e r D n J
r L I I D u I S R O e n L V t n D F h d e n I u e r d e n I
D O O Z e L V V J e t r R I I e n e n Y R r E e r e L t u n
J e n z u I u e h r e n P L t d e n D E D e n d e r u n J e
n d L e V L F h E e L P h e e r d u r F h d e n L n z Z L V
F h e n I D V t Y R O O e n d e t e n D u I P D r V F h e r
J e E e n D u I J D E e n Y e r t e L O X n J u n d R S e r
D t L R n V z L e O E O e L E e n u n Y e r D e n d e r t D
n J r L I I V t D J e r V t e r n e u n t e r n e u n z e h
n h u n d e r t n e u n u n d d r e L z L J D n J r L I I V
z e L t Y L e r u h r I u e n I u n d Y L e r z L J

Abb. 91. Fragmentarische Entzifferung mittels „neunzehnhundertneun"
Acht Zeichen sind vermutlich entziffert: d e h n r t u z

g e h e i P **e** N R P P D n d R V D F h e Z e i V u n g n r e
i n V f u e r d i e N r i e g V f u e h r u n g n D F h d e
P D O O e S R O i t i V F h e n P R e g O i F h N e i t e n
e r V F h R e S f t V i Q d u P D u f f r i e d O i F h e P
Z e g e e i n e f u e r **d e u t** V F **h** O D n d u n e r t r D
e g O i F h e O D g e D n V e i n e r R V t g r e n z e z u
E e V e i t i g e n h D E e i F h P i F h z u r g e Z D O t
V D P e n O R e V u n g e n t V F h O R V V e n d e r D n g
r i f f D u f S R O e n i V t n D F h d e n f u e r d e n f
D O O Z e i V V **g e t r** R **f f e n e n** v R r E e r e i t u n
g e n z u f u e h r e n P i t d e n D E D e n d e r u n g e
n d i e V i F h E e i P h e e r d u r F h d e n i n z Z i s
F h e n f D V t v R O O e n d e t e n D u f P D r V F h e r
g e E e n D u f g D E e n v e r t e i O u n g u n d R S e r
D t i R n V z i e O E O e i E e n u n v e r D e n d e r t D
n g r i f f V t D g e r V t e r n e u n t e r n e u n z e h
n h u n d e r t n e u n u n d d r e i z i g D n g r i f f V
z e i t v i e r u h r f u e n f u n d v i e r z i g

Abb. 92. Weitere fragmentarische Entzifferung mittels „vieruhrfuenfundvierzig"
Zwölf Zeichen sind vermutlich entziffert: d e f g h i n r t u v z

g e h e i m e N o m m a n d o s a c h e Z e i s u n g n o e
i n s f u e r d i e N r i e g s f u e h r u n g n a c h d e
m a O O e S o O i t i s c h e n m o e g O i c h N e i t e n
e r s c h o e S f t s i n d u m a u f f r i e d O i c h e m
Z e g e e i n e f u e r d e u t s c h O a n d u n e r t r a
e g O i c h e O a g e a n s e i n e r o s t g r e n z e z u
E e s e i t i g e n h a E e i c h m i c h z u r g e Z a O t
s a m e n O o e s u n g e n t s c h O o s s e n d e r a n g
r i f f a u f S o O e n i s t n a c h d e n f u e r d e n f
a O O Z e i s s g e t r o f f e n e n v o r E e r e i t u n
g e n z u f u e h r e n m i t d e n a E a e n d e r u n g e
n d i e s i c h E e i m h e e r d u r c h d e n i n z Z i s
c h e n f a s t v o O O e n d e t e n a u f m a r s c h e r
g e E e n a u f g a E e n v e r t e i O u n g u n d o S e r
a t i o n s z i e O E O e i E e n u n v e r a e n d e r t a
n g r i f f s t a g e r s t e r n e u n t e r n e u n z e h
n h u n d e r t n e u n u n d d r e i z i g a n g r i f f s
z e i t v i e r u h r f u e n f u n d v i e r z i g

Abb. 93. Letztes Zwischenergebnis
Siebzehn Zeichen sind vermutlich entziffert: a c d e f g h i m n o r s t u v z

g e h e i m e k o m m a n d o s a c h e w e i s u n g n o e
i n s f u e r d i e k r i e g s f u e h r u n g n a c h d e
m a l l e p o l i t i s c h e n m o e g l i c h k e i t e n
e r s c h o e p f t s i n d u m a u f f r i e d l i c h e m
w e g e e i n e f u e r d e u t s c h l a n d u n e r t r a
e g l i c h e l a g e a n s e i n e r o s t g r e n z e z u
b e s e i t i g e n h a b e i c h m i c h z u r g e w a l t
s a m e n l o e s u n g e n t s c h l o s s e n d e r a n g
r i f f a u f p o l e n i s t n a c h d e n f u e r d e n f
a l l w e i s s g e t r o f f e n e n v o r b e r e i t u n
g e n z u f u e h r e n m i t d e n a b a e n d e r u n g e
n d i e s i c h b e i m h e e r d u r c h d e n i n z w i s
c h e n f a s t v o l l e n d e t e n a u f m a r s c h e r
g e b e n a u f g a b e n v e r t e i l u n g u n d o p e r
a t i o n s z i e l b l e i b e n u n v e r a e n d e r t a
n g r i f f s t a g e r s t e r n e u n t e r n e u n z e h
n h u n d e r t n e u n u n d d r e i z i g a n g r i f f s
z e i t v i e r u h r f u e n f u n d v i e r z i g

Abb. 94. Endergebnis: „Weisung Nr. 1 für die Kriegsführung“

13.6 Maschinelle Exhaustion der Belegungen eines Musters

Helen Fouché Gaines schreibt, daß die Anfertigung von Listen von Wörtern gleichen Musters sehr nützlich sei, um auch die vertracktesten monoalphabetischen Substitutionen zu lösen.

13.6.1 Es darf angenommen werden, daß die professionellen Dienste dies schon lange wußten und spätestens seit der Verfügbarkeit von Rechenanlagen mit Magnetbandspeichern, also etwa ab 1955, auch praktisch nutzten. Es gibt neuerdings publizierte Tabellenwerke für Belegungen von Mustern im Englischen: 1971, 1972 Muster bis zu 12 Zeichen von *Jack Levine*, 1977, 1982, 1983 Muster bis zu 15 Zeichen von *Richard V. Andree*[4]. Bei der Aufschreibung verwendet man zweckmäßigerweise die Methode des '*Quick Index*' (KWIC, 'Key Word in Context'), wobei rechts und links überschießende Wortreste, durch Klammern abgesetzt, mitgedruckt werden. Ein Beispiel, für das Muster *12131*, zeigt Abb. 95. Beachte, daß anana(s) oder (r)okoko nicht zum Muster *12131*, sondern zum Muster *12121* gehört.

(m) acada (m)	ebene	(r) igidi (taet)	(l) oboto (mie)
(m) ahara (ni)	(l) edere (inband)	(n) ihili (smus)	(s) olomo (n)
(m) alaga	(v) eheme (nt)	(b) ikini	(d) oloro (sa)
(c) alama (ri)	(b) elebe (n)	(m) iliti (a)	(g) onoko (kken)
(p) alata (l)	(b) elege (n)	imiti (eren)	(m) onolo (g)
(m) alaya	(g) elege (n)	(l) imiti (eren)	(m) onopo (l)
(t) amara	eleme (nt)	(d) irigi (eren)	(m) onoto (n)
(p) anama	(t) eleme (trie)	(v) isiti (eren)	(t) opolo (gie)
(s) araba (nde)	(h) elene	(c) ivili (st)	(d) oxolo (gie)
(f) arada (y)	(s) elene	(d) ividi (eren)	
(k) araja (n)	(g) elese (n)	(d) ivisi (on)	(s) tatut
(c) arava (n)	eleve		
(k) atala (nien)	(h) exere (i)		(c) umulu (s)
(k) atara (kt)			

Abb. 95. Quick-Index-Auflistung von Wörtern mit dem Muster *12131*

Solche Sammlungen von Mustern können maschinell hergestellt werden mit Hilfe eines Lexikons der betreffenden Sprache. Dabei werden aber wortübergreifende Kontakte, darunter auch solche, die beim Unterdrücken des Zwischenraums entstehen, nicht erfaßt. Teilweise Abhilfe bringt die Aufnahme aller grammatikalischen Endungen. Besser ist es, eine Textbasis des betreffenden Genres zu verarbeiten — etwa ein ganzer Zeitungsjahrgang auf CD.

13.6.2 Maschinelle Unterstützung ist auch beim sukzessiven Auffinden von Mustern in einem Geheimtext und beim Vorführen passender Belegungen,

[4] *Richard V. Andree*, Pattern & Non-Pattern Words, Raja Press, Norman, Oklahoma.

etwa auf einem Bildschirm, angebracht.[5] Rechnerunterstützung ist insbesondere angebracht, wenn kein wahrscheinliches Wort verfügbar ist und kein Muster vorgegeben ist, aber seltene Muster oder wiederholte Muster herauszufinden sind. Wenn solche existieren — was voraussetzt, daß der Text genügend lang ist — führt dies fast sicher zu einem Einstieg. Selbstverständlich kann eine anschließende fragmentarische Entzifferung rechnergestützt erfolgen, mit geringer interaktiver Arbeit. Bei einem systematischen Vorgehen sucht man im Text möglichst solche Muster zu finden, die nicht allzuviele Belegungen erlauben, und wendet darauf die Exhaustionsmethode (12.5) an. Diese Methode der **Mustersuche**, die zunächst ohne Heranziehung der Intuition ('*ciphertext-only attack* arbeitet, ist ein erstes Beispiel einer '*pure cryptanalysis*'). Sie macht ein Angebot, das exhaustiv abgearbeitet werden muß. Sie wird nachfolgend zur Methode der **gekoppelten Mustersuche** verfeinert.

13.6.3 Beim Auffinden mehrerer Muster schließen sich häufig einige Belegungen gegenseitig aus. Dadurch wird der Suchraum verkleinert. Beispielsweise finden sich in dem Geheimtext

```
S E N Z E I S E J P A N O A I A O P A N C A H A O A J
                        1 2 3 2 1 4 2     1 2 1 3 1
```

die Muster *1232142* und *12131*; zu der in 13.3 verzeichneten Belegung s e m e s t e (r) für *1232142* passen aber nur wenige Belegungen für *12131*, nämlich nur solche, die mit e H e s e verträglich sind; das ist aus der Liste von Abb. 95 lediglich (g) e l e s e (n) . Zu der ebenfalls in frage kommenden Belegung g e r e g n e t für *1232142* passen nur solche Belegungen für *12131*, die mit e H e g e verträglich sind; das sind aus der Liste von Abb. 95 lediglich (g) e l e g e (n) und (b) e l e g e (n) . P $\hat{=}$ n aus der Belegung mit g e r e g n e t stößt sich aber mit J $\hat{=}$ n sowohl aus (g) e l e g e (n) wie auch aus (b) e l e g e (n) . Dieser Versuch bricht also bereits ab.

Dies zeigt, wie die beiden Muster *1232142* und *12132* zu einem einzigen

```
S E N Z E I S E J P A N O A I A O P A N C A H A O A J
                        1 2 3 2 1 4 2 5 6 2 7 2 1 2 8
```

vereinigt wurden.

Mit s e m e s t e r für *12321425* und g e l e s e n für *6272128* sind nun sieben Buchstaben festgelegt und das folgende Fragment erzielt:

S E r Z E m S E n t e r s e m e s t e r g e l e s e n

Für die Wahl der Klartextzeichen für S , E und Z verbleiben also $19 \cdot 18 \cdot 17 = 5814$ Möglichkeiten. Diese Zahl wird aber noch drastisch reduziert, wenn man die rund ein Dutzend Muster für S E n t e r aufsucht. Offen und der Intuition anheimgegeben bleibt sodann noch die Entzifferung von Z . Diese etwa

[5] Insbesondere wird man auch nach wiederholten Mustern im Geheimtext suchen, die womöglich (ja sogar „wahrscheinlich“) die selbe, häufiger vorkommende Klartextfloskel chiffrieren. Wir werden darauf („Parallelstellensuche“) in 17.4 zurückkommen.

$12 \cdot 17 \approx 200$ Fälle sind mit maschineller Unterstützung schnell überprüft. Angenommen, man fände neben der naheliegenden vollen Entzifferung

w i r d i m w i n t e r s e m e s t e r g e l e s e n

noch eine zweite oder diese Entzifferung würde angesichts der gegenüber der Unizitätslänge kurzen Länge des Textes (27) angezweifelt, so wäre im Sinne von *Rohrbach*s Forderung (13.3.1) ohnehin noch der Schlüssel aufzustellen, der sich für diese Entzifferung als ein CAESAR mit der Verschiebung $22 \simeq -4$ herausstellt. Das dürfte schließlich genügend glaubwürdig sein. Es sollte jedoch bemerkt werden, daß für die Entzifferung kein Gebrauch von den Besonderheiten einer CAESAR-Chiffrierung gemacht wurde.

13.6.4 Man sollte erwarten, daß in einem monoalphabetisch chiffrierten Geheimtext die Anzahl der vorkommenden Muster proportional der Länge ist; die Kopplung der Muster jedoch mindestens quadratisch mit der Länge anwächst, so daß die aus der Kopplung der Muster hervorgehenden Einschränkungen rasch zunehmen und den Suchraum der Exhaustion entsprechend einengen.

13.7 Pangramme

Nützlich sind ferner Listen von langen Wörtern, die keine wiederholten Buchstaben enthalten, also von der Form *123456789*...$\mathcal{N}$ sind (Pangramme[6], *non-pattern words*). Notwendigerweise gilt $\mathcal{N} \leq N$.

13.7.1 *Andree* zählt einige hundert Pangramme der Länge 11 wie

„abolishment“ „atmospheric“ „comradeship“ „exculpation“ „filamentous“ „hypogastric“ „nightwalker“ „questionary“ „slotmachine“ „spaceflight“

und einige Dutzend der Länge 12 wie

„ambidextrous“ „bakingpowder“ „bodysnatcher“ „disreputably“ „housewarming“ „hydrosulfite“ „springbeauty“ „talcumpowder“

auf. Sogar einige Pangramme der Länge 13 sind aufgelistet:

„bowstringhemp“ „doubleparking“ „doublespacing“ „groupdynamics“ „publicservant“

und eines der Länge 14:

„ambidextrously“

Beachte, daß in diesen Beispielen der Wortzwischenraum unterdrückt ist. Es gibt natürlich längere Pangramm-Sätze. Kommen solche Wörter oder Sätze im Klartext vor, erfordert der Einstieg nur eine Exhaustion von kleinem Umfang. Sie sollten also unterdrückt werden.

---

[6] *Richard V. Andree*, Nonpattern Words of 3 to 14 letters, Raja Press, Norman, Oklahoma 1982.

13.7.2 Echte Pangramme sind Sätze, die *jeden* Buchstaben genau einmal enthalten ($\mathcal{N} = N$). Im Deutschen ist kein echtes Pangramm bekannt, gute Approximationen sind

sylvia wagt quick den jux bei pforzheim (33 Zeichen),
bayerische jagdwitze von maxl querkopf (34 Zeichen) und
zwei boxkaempfer jagen eva quer durch sylt (36 Zeichen).

Im Englischen sind echte Pangramme (26 Zeichen) in sehr freier Sprache möglich, etwa

cwm, fjord-bank glyphs rest quiz (*Dmitri Borgmann*) und
squdgy fez, blank jimp, crwth vox (*Claude E. Shannon*).
Zing! Vext cwm fly jabs Kurd qoph (unbekannter Author).

Gute Approximationen sind im Englischen und Französischen

waltz, nymph, for quick jigs vex bud (28 Zeichen),
jackdaws love my big sphinx of quartz (31 characters),
pack my box with five dozen liquor jugs (32 Zeichen).
Qui, flamboyant, guida Zéphire sur ses eaux (35 Zeichen; Guyot, 1772).

Bekannt sind seit langem die Testtexte für Fernschreibverbindungen

kaufen sie jede woche vier gute bequeme pelze
the quick brown fox jumps over the lazy dog
voyez le brick geant que j'examine pres du wharf.

Für Vokal-Pangramme, in denen jeder Vokal genau einmal vorkommt, eignet sich besonders das Französische. Gute Annäherungen an echte Vokal-Pangramme sind *ultraviolet, trouvaille, autrefois, ossuaire, oripeau, ouaille* und *oiseau*, das den Vogel abschießt.

14 Polyalphabetischer Fall: Wahrscheinliche Wörter

14.1 Negative Mustersuche

Übereinstimmung von Mustern ist notwendigerweise auf monoalphabetische Chiffrierungen beschränkt. Für eine weite Klasse von polyalphabetischen, *endomorphen* Chiffrierungen, nämlich für solche, die der Bedingung genügen

in jedem Alphabet wird kein Zeichen durch das selbe Zeichen chiffriert

ist jedoch eine Negativsuche nach einem Muster angezeigt: Sie erlaubt eine Ausschließung derjenigen Lagen eines wahrscheinlichen Wortes, die die Bedingung irgendwo verletzen (einen 'Krach', engl. *crash* geben) und liefert damit mögliche Lagen. Die Ausschöpfung geht über die Länge des Textes und ist wie die Suche nach Wiederholungsmustern in Kapitel 13 machbar.

Die Vorbedingung, daß kein Zeichen durch sich selbst chiffriert wird, ist für polyalphabetische Chiffrierschritte häufiger erfüllt, als man auf den ersten Blick denken mag. Nicht nur gilt sie für alle echt involutorischen Permutationen (PORTA-Chiffrierschritte, 7.4.4, wobei $N = |V|$ gerade ist), sie gilt auch für alle voll zyklischen Permutationen (MULTIPLEX-Chiffrierschritte, 7.5.3). Für BEAUFORT-Chiffrierschritte (7.4.3) gilt sie dagegen nicht.

Monoalphabetische Chiffrierschrittsysteme vermeiden oft – in bester Absicht – Fixpunkte, für *aristocrats* (vgl. 13.3.2) ist das sogar vorgeschrieben. Wird ein polyalphabetisches Chiffrierschrittsystem aus mehreren monoalphabetischen Chiffrierschrittsystemen zusammengesetzt, vererbt sich diese Eigenschaft, die dann zu einer illusorischen Komplikation wird.

Die Nichtübereinstimmungsprüfung ergibt i.a. mehrere mögliche Lagen eines vermuteten Wortes (‚Treffer'), die exhaustiv zu untersuchen sind, ob sie echte Treffer oder Fehltreffer sind. Handelt es sich um ein Shannonsches Chiffrierschrittsystem (vgl. 2.6.4) und sind die Alphabete bekannt, so kann für einen echten Treffer ein Teil des Schlüssels rekonstruiert werden. Das mag einen Schlüssel mit bekanntem Konstruktionsprinzip vollständig bloßstellen, für einen periodischen Schlüssel sind weite Teile des Klartexts aufgedeckt. Die Nichtübereinstimmungsprüfung funktioniert selbstverständlich auch im monoalphabetischen Fall.

Für die Phrase „Erloschen ist Leuchttonne“ (vgl. 11.1.3) sind in nachfolgendem Chiffrat unter der angegebenen Bedingung nur zwei Lagen möglich, alle anderen führen zu einem ‘Krach’, der durch Fettdruck angezeigt wird:

YOAQUTHNCHWS YTI WHTOJ QMTCF KUS LZVS MF NGTDUQNYAVH

erlosc**h**enistleuc**ht**tonne
erloscheni**s**tleuchttonne
erloschenis**t**leuchttonne
erlos**ch**enistleuchttonne
erloschenistleucht**t**onne
erloschen**i**stleuch**t**tonne
erloschenis**t**leuchttonne
erlo**s**chenistleuchttonne
erloschenistleu**c**httonne
→ erloschenistleuchttonne
erlosc**h**enistleuchttonne
erloschenis**t**leuchttonne
erloschenistle**u**chttonne
erloschenistleuchtton**n**e
erloschenistleuchtto**n**ne
erl**o**schenistleuchttonne
erloschenist**l**euchttonne
erloscheni**s**tleuchttonne
erlos**c**henistleucht**t**onne
erloschenistleuch**t**ton**n**e
erloschenistleuchtto**n**ne
erloscheni**s**tleuchttonne
→ erloschenistleuchttonne

Eine Reihe maschineller Chiffrierverfahren sind gegen die Methode anfällig:

Erstens: Schieber- und Zylindergeräte (vgl. 7.5.3), deren Alphabete volle zyklische Permutationen sind.

Zweitens: Geräte, die „zur Erleichterung der Arbeitsweise“ involutorisch arbeiten. Dann ist jedes Alphabet eine involutorische Permutation. Werden aus technischen Gründen Zyklen der Länge 1 (Fixpunkte) ausgeschlossen, so ist wieder die Voraussetzung für die Negativsuche nach einem Muster gegeben.

Bei den mechanischen Chiffriermaschinen von *Hagelin* traf dies nicht zu; die BEAUFORT-Chiffrierschritte umfassen die Identität. Die ENIGMA aber litt unter dieser Schwachstelle gerade wegen der als besonders raffiniert gedachten Einführung der Umkehrwalze. Es fiele schwer, zu glauben, daß die über die Sicherheit der eigenen Systeme wachende Gruppe IV (*Hüttenhain*) der Chiffrierabteilung *Chi* des OKW *diese* Einbruchmöglichkeit nicht kannte oder unterschätzte. Jedenfalls war sie *ein* wesentlicher Bestandteil für die Arbeit des polnischen *Biuro Szyfrów* und der britischen Dechiffrierer in *Bletchley Park*. Aber die in der amerikanischen Kriegsmarine ebenso sorglos verwendete CSP-642, polyalphabetisch mit MULTIPLEX-Chiffrierschritten, war gleichermaßen gefährdet; die Japaner machten sich das zu nutze, nachdem sie auf den Inseln Wake und Kiska die Schiebergeräte erbeutet hatten.

Kurze Suchwörter erlauben selbstverständlich viele Treffer und ergeben damit auch viele Fehltreffer. Die Gesamt-Trefferwahrscheinlichkeit der Negativ-

n	$P(n)$ (in %)	n	$P(n)$ (in %)
1	96.15	12	62.45
2	92.45	16	53.39
3	88.90	24	39.01
4	85.48	32	28.51
5	82.19	48	15.22
6	79.03	64	8.13
8	73.07	96	2.32
10	67.56	128	0.66

Abb. 96. Gesamt-Trefferwahrscheinlichkeit der Negativ-Mustersuche $(N=26)$

suche nach einem Wort der Länge n ist $P(n) = (1 - 1/N)^n \asymp e^{-n/N}$. Abb. 96 zeigt einige Werte für den üblichen Fall $N = 26$.

Nachfolgender Klartext der Länge 60 (*Konheim*) ist ENIGMA-chiffriert:

```
manyo rgani zatio nsrel yonco mpute
GRSUZ TLDSZ NKWNE RDPFB OVVQN OBKYI

rsand datac ommun icati onsto keept
QNJRC QLIFR VTPKI LHGQV TMMJY MAJUJ
```

Bei der Negativsuche für das 8-Zeichen-Wort *computer* sollten für die ersten 26 Positionen ungefähr 19 $(26 \cdot 0.7307)$ mögliche Lagen auftreten. Tatsächlich sind hier 21 der Lagen nicht auszuschließen und damit gibt es 20 Fehltreffer:

```
  G R S U Z T L D S Z N K W N E R D P F B O V V Q N O B K Y I Q N J
  c o m p u t e r
  → c o m p u t e r
    → c o m p u t e r
      → c o m p u t e r
        → c o m p u t e r
          → c o m p u t e r
            → c o m p u t e r
              → c o m p u t e r
                  c o m p u t e r
                  → c o m p u t e r
                    → c o m p u t e r
                      → c o m p u t e r
                        → c o m p u t e r
                          → c o m p u t e r
                              c o m p u t e r
                              → c o m p u t e r
                                → c o m p u t e r
                                  → c o m p u t e r
                                    → c o m p u t e r
                                        c o m p u t e r
                                        → c o m p u t e r
                                          → c o m p u t e r
                                            → c o m p u t e r
                                             •→ c o m p u t e r
                                                  c o m p u t e r
                                                  → c o m p u t e r
```

/computer/ ist ein sehr kurzes Wort, /oberkommandoderwehrmacht/ (19.7.1) wäre da schon besser. Die Auszählung ergibt für die ersten 36 Positionen dieses 24-Zeichen-Worts 14 mögliche Lagen — alles Fehltreffer — gegenüber erwarteten $36 \cdot 0.3901 = 14.04$. Suchwörter von über 100 Zeichen wären gut geeignet: Für $n = 128$ und ein Textstück der Länge 300 ist $300 \cdot P(n) \approx 2$.

14.2 Binäre negative Mustersuche bei Porta-Alphabeten

Besonders günstige Voraussetzungen für eine negative Mustersuche liegen vor, wenn es sich um (polyalphabetische) Involutionen handelt, die nicht nur *einen* Buchstaben auslassen, sondern eine Hälfte des Alphabets in die andere abbilden und umgekehrt (PORTA-Chiffrierschritte, vgl. 7.4.4), etwa (Z_{26})

$$\{\mathrm{a\,b\,c\,d \ldots l\,m}\} \overset{2}{\longleftrightarrow} \{\mathrm{n\,o\,p\,q \ldots y\,z}\} \ .$$

Das **binäre Muster** eines Wortes erhält man, wenn man jedes Zeichen durch 0 oder 1 ersetzt, jenachdem ob es aus der ersten oder der zweiten Hälfte des Alphabets ist.

Angenommen, der selbe Text wie oben ist irgendwie PORTA-chiffriert:

```
m a n y o   r g a n i   z a t i o   n s r e l   y o n c o   m p u t e   r s a
P R G B F   I O Z G P   L Y C N E   E D G W S   A I K Q D   O B K J Q   C M P
```

/computer/ hat das binäre Muster 01011101 , deshalb ist im Geheimtext nach vollständiger Nichtübereinstimmung mit diesem Muster zu suchen:

```
P R G B F I O Z G P L Y C N E E D G W S A I K Q D O B K J Q C M P
1 1 0 0 0 0 1 1 0 1 0 1 0 1 0 0 0 0 1 1 0 0 0 1 0 1 0 0 0 1 0 0 1

0 1 0 1 1 1 0 1
  0 1 0 1 1 1 0 1
    0 1 0 1 1 1 0 1
      0 1 0 1 1 1 0 1
        0 1 0 1 1 1 0 1
          0 1 0 1 1 1 0 1
            0 1 0 1 1 1 0 1
              0 1 0 1 1 1 0 1
                0 1 0 1 1 1 0 1
                  0 1 0 1 1 1 0 1
                    0 1 0 1 1 1 0 1
                      0 1 0 1 1 1 0 1
                        0 1 0 1 1 1 0 1
                          0 1 0 1 1 1 0 1
                            0 1 0 1 1 1 0 1
                              0 1 0 1 1 1 0 1
                                0 1 0 1 1 1 0 1
                                  0 1 0 1 1 1 0 1
                                    0 1 0 1 1 1 0 1
                                      0 1 0 1 1 1 0 1
                                        0 1 0 1 1 1 0 1
                                          0 1 0 1 1 1 0 1
                                            0 1 0 1 1 1 0 1
                                      ●→      0 1 0 1 1 1 0 1
                                                0 1 0 1 1 1 0 1
                                                  0 1 0 1 1 1 0 1
```

In diesem Beispiel führt die Nichtübereinstimmungsprüfung – bei erwarteten $26 \cdot (\frac{1}{2})^8 = 0.102$ möglichen Lagen – zu keinem Fehltreffer, im Gegensatz zu 20 Fehltreffern vorhin, mit einem ebenso kurzen Wort. Sogar das noch kürzere 4-Zeichen-Wort /comp/ mit dem binären Muster 0101 hat nur drei Fehltreffer – gegenüber erwarteten $26 \cdot (\frac{1}{2})^4 = 1.62$ möglichen Lagen. Im allgemeinen sind bei PORTA-Chiffrierungen wahrscheinliche Wörter mit einigen wenigen Zeichen schon ausreichend, um eindeutig zwischen einem echten Treffer oder dem Nichtvorkommen zu unterscheiden.

Daß das aus /oberkommandoderwehrmacht/ herrührende 11-Zeichen-Wort /kommandoder/ mit dem Muster

01000101001

im Klartext dieses Beispiels nicht vorkommen kann, zeigt sich sogleich, da jede Lage zu einem 'Krach' führt:

```
P R G B F I O Z G P L Y C N E E D G W S A I K Q D O B K J Q C M P
1 1 0 0 0 0 1 1 0 1 0 1 0 1 0 0 0 0 1 1 0 0 0 1 0 1 0 0 0 1 0 0 1
0 1 0 0 0 1 0 1 0 0 1
  0 1 0 0 0 1 0 1 0 0 1
    0 1 0 0 0 1 0 1 0 0 1
      0 1 0 0 0 1 0 1 0 0 1
        0 1 0 0 0 1 0 1 0 0 1
          0 1 0 0 0 1 0 1 0 0 1
            0 1 0 0 0 1 0 1 0 0 1
              0 1 0 0 0 1 0 1 0 0 1
                0 1 0 0 0 1 0 1 0 0 1
                  0 1 0 0 0 1 0 1 0 0 1
                    0 1 0 0 0 1 0 1 0 0 1
                      0 1 0 0 0 1 0 1 0 0 1
                        0 1 0 0 0 1 0 1 0 0 1
                          0 1 0 0 0 1 0 1 0 0 1
                            0 1 0 0 0 1 0 1 0 0 1
                              0 1 0 0 0 1 0 1 0 0 1
                                0 1 0 0 0 1 0 1 0 0 1
                                  0 1 0 0 0 1 0 1 0 0 1
                                    0 1 0 0 0 1 0 1 0 0 1
                                      0 1 0 0 0 1 0 1 0 0 1
                                        0 1 0 0 0 1 0 1 0 0 1
                                          0 1 0 0 0 1 0 1 0 0 1
                                            0 1 0 0 0 1 0 1 0 0 1
```

14.3 Mustersuche bei bekannten Alphabeten – De Viaris

Für Schieber- und Zylindergeräte mit (voll zyklischen) unabhängigen Alphabeten, für die nach 14.1 bereits die negative Mustersuche möglich ist, kann der unbefugte Entzifferer noch mehr tun. Dies mußte *Étienne Bazeries*, der große Praktiker der Kryptologie, schmerzlich erfahren, als das von ihm für unüberwindlich gehaltene Zylindergerät von seinem Gegenspieler *de Viaris* (vgl. 7.5.3) bloßgestellt wurde. Die Methode von *de Viaris* 1893 und *Friedman* 1918 setzt übrigens nicht voraus, daß die Alphabete voll zyklisch oder echt involutorisch sind.

14.3.1 Auch die allgemeine Methode setzt aber nun den Besitz des Gerätes voraus. Da die Anzahl der Scheiben oder Lineale systemmäßig keiner Beschränkung unterliegt, ist die Anzahl der jeweiligen Anordnungen immer als groß genug anzusehen, um eine Exhaustion auszuschließen. Die Periode ist systemmäßig festgelegt; die bekannten Alphabete könnten also gegen Kolonnen monographisch chiffrierter Zeichen geprüft werden (s. 18.2.5); aber das Material reicht oft nicht aus, um eine Häufigkeitsanalyse durchzuführen.

Für den speziellen Fall der Schieber- und Zylindergeräte kommt die scheinbare Komplikation der Entzifferung durch die Polyphonie des Verfahrens hinzu. Angenommen, die Chiffre sei (homophon) in der k-ten Zeile nach dem eingestellten Klartext-Stück (in der k-ten Generatrix, vgl. 7.5.3) abgelesen worden. Man wird regelmäßig mit kleinen Werten von k beginnen und hat schlimmstenfalls zwei Dutzend Fälle durchzuprobieren. Ferner sei einfachheitshalber angenommen, ein wahrscheinliches Wort oder Textstück sei kurz genug, um nicht zerrissen zu werden.

Nun wird für ein bestimmtes wahrscheinliches Wort und ein gegebenes k festgestellt, welche Zeichen in der k-ten Generatrix auf der i-ten Scheibe oder dem i-ten Lineal stehen. Mit dieser Information fährt man am Geheimtext entlang und stellt fest, welche Lagen ihn überhaupt ergeben konnten. Ist das wahrscheinliche Wort kurz, so erhält man womöglich mehrere Möglichkeiten, die exhaustiv weiterzubehandeln sind. Ist das wahrscheinliche Wort lang, so ergibt sich vielleicht gar keine Möglichkeit; dann ist zu einer anderen Generatrix überzugehen. Gelingt es für keine Generatrix, so kommt das wahrscheinliche Wort, entgegen der Annahme, nicht vor – oder es wurde zerrissen.

Am Beispiel des Zylinders von *Bazeries* sei das Verfahren geschildert, mit einem Geheimtext, der auf Angaben von *Givierge* zurückgeht:

F S A M C R D N F E Y H L O E R T X V Z
L R M Q U U X R G Z N B O M L N D N P V
R T M U K H R D O X L A X O D C R E E H
V R E X Z G U G L A B S E S T V F N G H

Als wahrscheinliches Wort sei /division/ angenommen. Zu den 20 Zyklen von *Bazeries* (7.5.3, Abb. 56) ergeben sich (für die erste Generatrix) in Abb. 97 links in den sieben Spalten die Bildmengen der Klartextzeichen /d/, /i/, /v/, /i/, /s/, /i/, /o/, /n/ von /division/. Schiebt man jetzt einen Papierstreifen mit dem Geheimtext an diesen Bildmengen entlang, so kann man für jede Lage des wahrscheinlichen Wortes feststellen, ob die sämtlichen Chiffrenbuchstaben für dieses Wort unter den verfügbaren zu finden sind. Beispielsweise ist das nicht der Fall für die folgende Lage

F S A **M** **C** **R** D N F E Y H L O E R T X V Z
d i v i s i o n

bei der sich (in der 1. Generatrix) nur die vier fettgedruckten Chiffren (statt der erwünschten acht) wiederfinden. Auch für die nächste Lage

	d	i	v	i	s	i	o	n
1	E	J	X	J	T	J	P	O
2	F	O	X	O	T	O	U	P
3	F	O	X	O	T	O	J	P
4	C	H	U	H	R	H	N	M
5	C	Q	T	Q	R	Q	I	M
6	C	E	T	E	R	E	I	M
7	P	J	B	J	E	J	N	S
8	T	E	D	E	P	E	Y	H
9	E	J	X	J	L	J	P	O
10	I	E	X	E	V	E	T	C
11	B	T	I	T	**C**	T	U	D
12	G	C	Y	C	A	C	R	P
13	N	R	Y	R	A	**R**	I	S
14	**F**	B	X	B	V	B	N	E
15	F	N	X	N	T	N	P	S
16	K	M	X	**M**	V	M	G	F
17	F	E	X	E	O	E	N	A
18	I	U	X	U	T	U	M	Q
19	F	J	L	J	U	J	N	T
20	G	J	X	J	T	J	U	O

	d	i	v	i	s	i	o	n
1	**H**	M	A	M	X	A	S	R
2	J	B	E	B	Z	B	E	S
3	I	**L**	E	L	Z	L	M	Q
4	Z	E	R	**E**	O	E	K	J
5	U	M	**O**	M	Q	M	N	E
6	U	X	Q	X	N	X	Z	J
7	J	V	K	V	D	V	F	T
8	M	U	J	U	D	U	F	X
9	L	N	H	N	I	N	V	U
10	P	R	D	R	Z	R	A	J
11	**H**	S	L	S	**R**	S	N	G
12	K	B	R	B	U	B	Z	**V**
13	U	T	L	T	B	**T**	M	X
14	K	F	H	F	Z	F	R	T
15	K	R	N	R	E	R	**X**	U
16	S	O	J	O	Z	O	R	H
17	J	O	Y	O	B	O	C	D
18	B	C	L	C	U	C	R	Y
19	J	Q	F	Q	M	Q	Z	A
20	J	P	N	P	A	P	E	T

Abb. 97. Bildmengen von /division/ ,
links 1. Generatrix (mit **F**SA**MCR**DN) , rechts 4. Generatrix (mit **HLOERTXV**)

F S A M **C** **R** D **N** **F** E Y H L O E R T X V Z
d i v i s i o n

finden sich (in der 1. Generatrix) nur die vier fettgedruckten Chiffren (statt acht) wieder. Für die übernächste Lage

F S A **M** C **R** D **N** F **E** Y H L O E R T X V Z
d i v i s i o n

sieht es nicht besser aus. So kann man fortfahren und für alle weiteren Lagen von /division/ die 1. Generatrix ausschließen.
Nun wendet man sich einer anderen Generatrix zu. Abb. 97 rechts zeigt für die 4. Generatrix die Bildmengen von /division/ mit den gleichen 20 Alphabeten. Beginnt man wieder ganz links, so ergibt sich erstmals für die Lage

F S A M C R D N F E Y **H** **L** **O** **E** **R** **T** **X** **V** Z
d i v i s i o n

ein Treffer: Alle acht (fettgedruckten) Chiffren sind in der Bildmenge, und sieben von ihnen finden sich sogar nur einmal, legen also das zugehörige Alphabet fest. Lediglich für **H** hat man, wie Abb. 97 rechts zeigt, die Qual der Wahl zwischen dem ersten und dem elften Alphabet.

14.3.2 An dieser Stelle geht eine weitere Kenntnis über das System in die Kryptanalyse ein. Prinzipiell könnte auch ein unabhängiges Alphabet, so wie begleitende Alphabete, mehrfach verwendet werden. Für Zylinder- und Schiebergeräte gilt aber üblicherweise, daß jede Scheibe bzw. jedes Lineal nur einmal vorhanden ist und innerhalb der Periode genau einmal verwendet wird. Dieser Bedingung entspräche bei VIGENÈRE-Schritten, daß im Schlüsselwort jedes Zeichen nur einmal vorkommt. Während es dort dafür sorgt, daß die Alphabete der einzelnen Kolonnen nicht kumuliert werden

(‚progressive Chiffrierung‘, 8.4.2), liegt hier, sobald die Alphabete in Feindeshand gefallen sind, offensichtlich eine *complication illusoire* vor.

Unter der insbesondere für den Zylinder von *Bazeries* geltenden Annahme kann nun für H ≙ d das elfte Alphabet ausgeschlossen werden, da es bereits eindeutig für R ≙ s benötigt wird. Also ergibt sich die folgende Anordnung von acht der 20 Zylinder

```
* * * * *   * * * * *   * 1 3 5 4   11 13 15 12 *
```

Sollte das kein Fehltreffer sein, so müßte sich im Abstand von 20 Zeichen jeweils wieder eine Entzifferung ergeben. Man erhält für die Lage

```
L R M Q U   U X R G Z   N B O M L   N D N P V
                          1 3 5 4   11 13 15 12
                          z h p n   r m y k       24.
                          a i n m   a t i n       ←
                          B O M L   N D N P       1.
                          c j l k   d n s q       2.
                          d k k j   b s t t       3.
```

eine überzeugende Entzifferung /ainmatin/ : Für diese Runde wurde also die 1. Generatrix benutzt. Weiterhin erhält man im Abstand von 40 Zeichen

```
R T M U K   H R D O X   L A X O D   C R E E H
                          1 3 5 4   11 13 15 12
                          A X O D   C R E E       22.
                          b z i c   o e z z       23.
                          c a q b   u m l l       24.
                          d e p a   r t a s       ←
                          e b n z   a d j a       1.
```

die überzeugende Entzifferung /departas/ , es wurde also für diese Runde die 22. Generatrix benutzt. Die Polyphonie macht keine Schwierigkeiten mehr.

/departas/ kann man nun auf zweierlei Weise ergänzen: zu /departasixheures/ oder zu /departaseptheures/ . Bedenkt man, daß 6 Uhr für die französische Armee schrecklich früh wäre, so wird man es vielleicht zunächst versuchen mit /departaseptheures/ als wahrscheinlichem Wort, das zerrissen wird in /departase/ und /ptheures/ . Letzteres ergibt in der unmittelbar anschließenden Lage (die Bildmenge von /ptheures/ mit der 3. Generatrix zeigt Abb. 98, die Chancen für einen Fehltreffer stehen 1:206) den Treffer

V R E X Z   G U G L A   B S E S T   V F N G H
p t h e u   r e s

der auch die Position von vier weiteren, nicht verbrauchten Zylindern festlegt: R ≙ t erfordert den 7., X ≙ e den 6., G ≙ r den 10., G ≙ s den 9. Zylinder. In Abb. 98 sind die bisher bestimmten Zylinder markiert. Von den verbleibenden verlangt nunmehr Z ≙ u eindeutig den 17. Zylinder, während drei Fälle offen bleiben: ob zu V ≙ p der 16. oder der 20. Zylinder gehört, zu E ≙ h der 14. oder der 18. Zylinder, zu U ≙ e der 2. oder der 8. Zylinder.

		p	t	h	e	u	r	e	s
●	1	S	X	K	H	Y	U	H	V
	2	S	Z	L	U	C	V	**U**	X
●	3	Q	Z	J	D	R	V	D	X
●	4	M	Q	**E**	B	R	O	B	P
●	5	L	O	D	H	V	Q	H	I
●	6	L	Q	D	**X**	E	N	X	P
●	7	J	**R**	Q	D	B	U	D	T
	8	D	M	X	U	L	S	**U**	V
●	9	**V**	F	Y	L	**Z**	D	L	**G**
●	10	T	A	M	R	O	**G**	R	Y
●	11	Y	S	M	T	N	D	T	U
●	12	**V**	F	N	S	D	Z	S	C
●	13	Y	S	P	D	C	T	D	X
	14	B	I	**E**	T	P	A	T	Y
●	15	X	E	O	A	L	Z	A	U
	16	**V**	B	C	G	D	U	G	Y
	17	U	X	P	O	**Z**	L	O	A
	18	T	U	**E**	S	C	D	S	I
	19	S	A	B	C	M	X	C	Y
	20	**V**	A	K	C	E	Y	C	L

Total probability of hit

$$\frac{12}{25} \times \frac{13}{25} \times \frac{14}{25} \times \frac{13}{25} \times \frac{13}{25} \times \frac{14}{25} \times \frac{13}{25} \times \frac{11}{25}$$

$$\approx 1 : 206$$

$\mathrm{e} \mapsto \{A, B, C, D, G, H, L, O, R, S, T, U, X\}$

$\mathrm{h} \mapsto \{B, C, D, E, J, K, L, M, N, O, P, Q, X, Y\}$

$\mathrm{p} \mapsto \{B, D, J, L, M, Q, S, T, U, V, X, Y\}$

$\mathrm{r} \mapsto \{A, D, G, L, N, O, Q, S, T, U, V, X, Y, Z\}$

$\mathrm{s} \mapsto \{A, C, G, I, L, P, T, U, V, X, Y\}$

$\mathrm{t} \mapsto \{A, B, E, F, I, M, O, Q, R, S, U, X, Z\}$

$\mathrm{u} \mapsto \{A, B, E, F, I, M, O, Q, R, S, U, X, Z\}$

Abb. 98. Bildmengen von /ptheures/ , 3. Generatrix (mit **VREXZGUG**)

Es ergibt sich folgende Verteilung von 19 der 20 Zylinder

$$\tfrac{16}{20} \quad 7 \quad \tfrac{14}{18} \quad 6 \quad 17 \quad 10 \quad \tfrac{2}{8} \quad 9 \quad * \quad * \quad * \quad 1 \quad 3 \quad 5 \quad 4 \quad 11 \quad 13 \quad 15 \quad 12 \quad *$$

Die restliche Entzifferung ist eine Kleinigkeit; die bereits festgestellte Anordnung von 13 der Zylinder gibt die fragmentarische Entzifferung

```
F S A M C   R D N F E   Y H L O E   R T X V Z
* a * r o   i * i * *   * d i v i   s i o n *

L R M Q U   U X R G Z   N B O M L   N D N P V
* p * r t   e * a * *   * a i n m   a t i n *

R T M U K   H R D O X   L A X O D   C R E E H
* r * e i   m * s * *   * d e p a   r t a s e

V R E X Z   G U G L A   B S E S T   V F N G H
p t h e u   r e s * *   * p x x x   x x x x *
```



Marquis de Viaris (1847–1901)

in der weitere Bruchstücke /la troisieme/ , /demain/ sofort ergänzt werden können und alle Positionen bis auf die 20. festlegen. Für diese verbleibt dann der 14. Zylinder. Die komplette Reihenfolge der Zylinder, der Schlüssel, kann so zu

16 7 18 6 17 10 8 9 20 19 2 1 3 5 4 11 13 15 12 14

rekonstruiert werden und liefert (beachte die auffüllenden Blender am Ende)

```
F S A M C   R D N F E   Y H L O E   R T X V Z
l a t r o   i s i e m   e d i v i   s i o n s

L R M Q U   U X R G Z   N B O M L   N D N P V
e p o r t   e r a d e   m a i n m   a t i n s

R T M U K   H R D O X   L A X O D   C R E E H
u r r e i   m s s t o   p d e p a   r t a s e

V R E X Z   G U G L A   B S E S T   V F N G H
p t h e u   r e s s t   o p x x x   x x x x x
```

14.3.3 Auch beim Fehlen eines wahrscheinlichen Wortes ist die periodische polyalphabetische Chiffrierung mit bekannten, unabhängigen Alphabeten angreifbar: *Givierge* (1925) folgend, zieht man häufige Bigramme, Trigramme und Tetragramme heran. Wir zeigen das am Beispiel der französischen und englischen Allerweltsendung /ation/. Für jede Generatrix und für jedes Klartextzeichen wird die Menge der zugehörigen Geheimtextzeichen vorfabriziert. In Abb. 99 findet man für die erste Generatrix die Bildmengen; die Chancen stehen 1:51, Fehltreffer sind also noch recht selten zu erwarten.

	a	t	i	o	n
1	B	U	J	P	O
2	E	V	O	U	P
3	E	V	O	J	P
4	Z	S	H	N	M
5	J	S	Q	I	M
6	Z	S	E	I	M
7	L	D	J	N	S
8	V	O	E	Y	H
9	R	S	J	P	O
10	F	G	E	T	C
11	N	Z	T	U	D
12	I	V	C	R	P
13	U	D	R	I	S
14	I	P	B	N	E
15	J	R	N	P	S
16	I	H	M	G	F
17	B	U	E	N	A
18	B	D	U	M	Q
19	C	E	J	N	T
20	C	E	J	U	O

Total probability of hit

$$\frac{12}{25} \times \frac{11}{25} \times \frac{12}{25} \times \frac{10}{25} \times \frac{12}{25}$$

$$\approx 1 : 51$$

$$\text{a} \mapsto \{\text{B, C, E, F, I, J, L, N, R, U, V, Z}\}$$
$$\text{t} \mapsto \{\text{D, E, G, H, O, P, R, S, U, V, Z}\}$$
$$\text{i} \mapsto \{\text{B, C, E, H, J, M, N, O, Q, R, T, U}\}$$
$$\text{o} \mapsto \{\text{G, I, J, M, N, P, R, T, U, Y}\}$$
$$\text{n} \mapsto \{\text{A, C, D, E, F, H, M, O, P, Q, S, T}\}$$

Abb. 99. Bildmengen von /ation/, 1. Generatrix

Sowohl die Technik von *de Viaris* und *Friedman* wie die letzterwähnte von *Givierge*, die versuchen, viele kleine Inseln zu finden und zusammenzuschließen, sind mit Arbeitsplatzrechnern leicht mechanisierbar. Nicht ohne Stolz bemerkt *Givierge*, daß man sich dank eines ≪*mot probable*≫ Quintillionen von Versuchen ersparen kann.

14.3.4 Die allgemeine Methode von *de Viaris* zur Einengung des Suchraums setzt, wie oben gesagt, nicht voraus, daß die Alphabete voll zyklisch oder echt involutorisch sind. Sie hat aber mit der negativen Mustersuche nach 14.1 und 14.2 gemeinsam, daß systematisch untersucht wird, welche Menge von Geheimtextzeichen zusammen mit einem Klartextzeichen auftreten kann. Für den Entzifferer ist es umso besser, je kleiner diese Menge ist. Andrerseits bricht dieses Vorgehen und damit auch die allgemeine de Viaris-Methode zusammen, wenn jede der Mengen die volle Menge der Klartextzeichen ist. Dies erfordert eine besonders sorgfältige Zusammenstellung der Alphabete. Ein Chiffrierschrittsystem mit dieser defensiven Eigenschaft nennen wir ein **transitives** Chiffrierschrittsystem. Notwendigerweise ist dann die Anzahl der Alphabete größer oder gleich N. Dies war bei *Bazeries* Zylinder verletzt. Die M-138-A der U.S.A. benutzte 30 Lineale, die aus 50 oder 100 wechselnd ausgewählt wurden, und man kann erwarten daß die Auswahl stets so geschah, daß ein transitives Chiffrierschrittsystem entstand.

Die Anzahl der Alphabete ist kleiner oder gleich N, wenn die Shannon-Eigenschaft (2.6.4) vorliegt, daß jedes Paar von Klartext- und Geheimtextzeichen das Alphabet eindeutig festlegt. Für ein transitives Shannonsches MULTIPLEX-Chiffriersystem hat man also N Alphabete von je N Zeichen, sie bilden ein lateinisches $N \times N$-Quadrat (7.5.4). Die M-94 der U.S.A., mit 25 MULTIPLEX-Schritten, hatte Alphabete, die, zusammen mit der Identität, (fast) ein lateinisches 26×26-Quadrat bilden (7.5.4, Tabelle 2).

14.3.5 Der französische Marquis *Gaëtan Henri Léon de Viaris* (gallisierter *di Lesegno*) wurde am 13. Februar 1847 in Cherbourg geboren, sein Vater war Artilleriehauptmann. Mit 19 Jahren kam *de Viaris* auf die berühmte *École Polytechnique.* Mit 21 ging er zur See, später wurde er Polizeipräfekt und schließlich Infanterieoffizier. Sein Interesse für die Kryptologie erwachte um 1885; er betätigte sich zuerst als Erfinder einer der ersten druckenden Chiffriermaschinen. Sicherlich war er nach *Babbage* der erste, der mathematische Beziehungen in der Kryptologie einsetzte, nämlich 1888 bei der Charakterisierung linearer Substitutionen in einer Reihe von Artikeln. 1893 schrieb er dann die kryptanalytische Abhandlung *L'art de chiffrer et déchiffrer les dépêches secrètes*, die ihn berühmt machte. 1898 publizierte er auch einen kommerziellen Code. Er starb am 18. Februar 1901.

Marcel Givierge baute als Major beim Ausbruch des 1. Weltkriegs eine Entzifferungsabteilung des französischen Generalstabs auf. 1925, als sein Buch *Cours de Cryptographie* erschien, war er Oberst; er wurde später zum General befördert.

Unter Givierge arbeitete *George Jean Painvin*, ein genialer Entzifferer und vielseitiger Mann, der Paläontologie studiert hatte und nach dem 1. Weltkrieg ein bedeutender Wirtschaftsführer wurde.

14.3.6 In der besonderen Situation im Nachkriegsdeutschland, als der *FIAT Review of German Science* geschrieben wurde, konnte es geschehen, daß es zu einem der wenigen offenen und erhellenden Berichten über erfolgreiche kryptologische Aktivitäten hoheitlicher Dienste kam. In der Reihe über Angewandte Manthematik berichtete *Hans Rohrbach* über Kryptologie und gab tiefe Einblicke in die ‚Chiffrierphilosophie' der deutschen Seite; da er umfassend berichtete, gibt er indirekt auch Aufschluß über deren Lücken im kryptologischen, insbesondere im kryptanalytischen Kenntnisstand.

Rohrbach publizierte 1979 einen 1945 verfaßten Bericht, der im Detail schildert, wie systematisch und umfassend ab November 1943 eine MULTIPLEX-Chiffrierung, nämlich die ‚American Strip Cipher O-2' (wie er es nennt) – eine Version der M-138-A für den Diplomatischen Dienst der U.S.A. – gebrochen wurde durch eine Gruppe („Sonderdienst Dahlem") im Auswärtigen Amt, Pers Z, unter maßgeblicher Mitwirkung der Mathematiker *Werner Kunze*, *Hans Rohrbach*, *Annelise Hünke*, *Erika Pannwitz*, *Hansgeorg Krug*, *Helmut Grunsky* – Linguisten wie *Hans-Kurt Müller*, *Asta Friedrichs*, *Joachim Ziegenrücker*, *Ottfried Deubner* nicht zu vergessen. Wie *Rohrbach* berichtete,

begann die Arbeit mit der Sammlung und Aufbereitung eines umfangreichen aufgefangenen Spruchmaterials, hauptsächlich aus der und in die U.S.-Botschaft in Bern, wo *Allen W. Dulles* (*Office of Strategic Services*) residierte. Dabei fiel auf

1. das häufige Vorkommen von Parallelen, auch längeren, aber nie über mehr als 30 Zeichen gehend und häufig mit dem 15. Zeichen abbrechend,
2. das gehäufte Vorkommen von Parallelen in Sprüchen des selben Tages, jedoch nie in zwei Sprüchen an verschiedenen Tagen des selben Monats,
3. das Nichtvorkommen von Parallelen zwischen einem Spruch vor und einem Spruch nach dem 1. August 1942.

Man zog daraus den Schluß, daß immer 15 Zeichen (eine ‚Linie') in der gleichen Weise chiffriert wurden (Periode 15), gelegentlich sogar 30 Zeichen; daß der Schlüssel täglich wechselte, aber mehrfach verwendet werden konnte, und daß am 1. August das Chiffriersystem grundlegend geändert worden war.

Als Arbeitshypothese durfte also eine polyalphabetische Chiffrierung der Periode 15 angenommen werden, und zwar vermutlich keine polygraphische. Es war anzunehmen, daß insgesamt mehr als 15 Alphabete, vermutlich 30, zur Verfügung standen.

Bekannt war ferner eine Vorliebe der U.S.-Dienste für Zylinder- und Schiebergeräte. *Rohrbach* kannte aber die Alphabete nicht, ein klassischer de Viaris-Angriff wäre nicht möglich gewesen.

Untersuchungen unter Einsatz von Hollerith-Tabelliermaschinen ergaben

4. wenn die Nachrichten in Blöcke (‚Linien') von 15 Zeichen zerlegt wurden, erschienen alle Parallelen mit einer Länge von mindestens 8 Zeichen vertikal untereinander, also in den selben Positionen (‚phasenrein').

Dies bestätigte die Annahme einer monographischen polyalphabetischen Chiffrierung der Periode 15; überdies führte die Annahme, daß sich stereotype Floskeln ('From Murphy', 'Strictly Confidential') am Anfang fanden, zu der Vermutung, kein Buchstabe ginge in sich über, und zwei identische Klartextbruchstücke in der selben Periodenlage ergäben nicht den selben Geheimtext. Dies alles mündete in den Verdacht, daß eine polyphone Chiffrierung mit MULTIPLEX-Chiffrierschritten vorlag und keine Maschinenchiffrierung. Somit mußten für jeden Tag 15 oder 30 Alphabete rekonstruiert werden.

Die Ernte war allerdings, dank der Mitteilsamkeit der U.S. Botschaft in Bern, mit täglich durchschnittlich 15 Nachrichten aus durchschnittlich 40 Blöcken von 15 Zeilen, mehr als reichlich. Die Blöcke (‚Linien') mußten zuerst in ‚Familien' gruppiert werden. Eine ‚Familie' bestand aus allen Sprüchen mit gleichem Schlüssel, die also mit ein und demselben Satz von Alphabeten in gleicher Anordnung – vermutlich aus mehr als 15 ausgewählt – chiffriert waren. Zu einer ‚Klasse' wurden zusammengefaßt die 25 Familien, die den 25 verschiedenen Generatrizen ($N = 26$) entsprachen. Unter massivem Einsatz von Lochkartenmaschinen und von Sonderanfertigungen, worum sich besonders *Krug* verdient machte, wurde in kleinen Schritten das Material zu

Familien verdichtet und diese in Klassen eingeteilt; die umfangreichste dieser Klassen (Klasse III) mit ungefähr 3 000 Linien umfaßte 25 Familien mit je 60 bis 150 Linien. Man fand zunächst roh knapp 50 Klassen, am Ende war das gesamte Material genau 40 verschiedenen Klassen zugeordnet, wobei nur wenig Material, von Tagen mit geringem Verkehr stammend, unberücksichtigt bleiben mußte. Die Rekonstruktion der Alphabete einer solchen Klasse setzte dann an phasenreinen Bigramm- und Trigrammparallelen zwischen den Linien an, in geradliniger Fortsetzung der Überlegungen von *Givierge*. Der Einbruch gelang über das häufig vorkommende Tetragramm /tion/ und das Pentagramm /ation/, unterstützt von den Bigramm-Drillingen /in/, /an/, /on/ und /in/, /an/, /un/. *Rohrbach* beschreibt eindringlich, wie langsam Keime der Lösung durchschimmerten, wie sich dann Lücken füllen ließen und schließlich das Unternehmen „aus eigener Kraft“ lief. Der Erfolg war garantiert, als die ersten 2×15 Alphabete, nämlich die der Klasse III, bestimmt waren. Die Betrachtung anderer Klassen brachte eine Erweiterung auf insgesamt 50 Alphabete, die vollständig bestimmt wurden, dazu traten die 40 schließlich festgestellten Tagesschlüssel – man weiß heute, daß dies den Fakten entsprach.

So konnte schließlich alles aufgefangene Material der Geräte O-2 entziffert werden konnte. Um dies zu beschleunigen (von Hand konnte eine Person pro Schicht knapp 100 Linien bewältigen), baute *Kunze* eine halbautomatische Vorrichtung, die dem Auswerter das Einstellen der Streifen abnahm; er hatte nur noch die richtige Generatrix zu finden. Damit war es möglich, das gesamte Material innerhalb eines Monats zu entziffern. Leider ging, je besser es klappte, umso weniger neues Material ein: Mitte 1944 stellte das State Department auf ein moderneres und sichereres Chiffrierverfahren mittels der von der U.S.Army gelieferten SIGTOT-Maschinen mit individuellem Schlüssel um. Außerdem mußte der Sonderdienst Dahlem erst vor dem Bombenterror in Berlin und dann vor der nach Schlesien vorrückenden Sowjetarmee flüchten. Nicht besser erging es übrigens dem „Forschungsamt“ des Reichsluftfahrtministeriums, *Göring*s Abhördienst.

Die Japaner versuchten sich auch an der CSP-642, waren aber nicht sehr erfolgreich: *Kahn* meint, sie hätten *de Viaris*, *Friedman* (und *Givierge*) genauer studieren sollen. Wieviel den Russen gelang, ist unbekannt.

14.4 Zick-Zack-Exhaustion möglicher Wortlagen

Wird bei einem polyalphabetischen Verfahren ein Schlüssel in verständlicher Sprache verwendet, so darf man erwarten, daß es auch darin ‚wahrscheinliche Wörter‘ gibt. Damit besteht eine weitere Angriffsmöglichkeit: Die möglichen Lagen eines im Schlüssel vermuteten Wortes sind dadurch bestimmbar, daß die Dechiffrierung des Geheimtextes mit diesem Schlüsselbruchstück einen vernünftigen Klartext ergibt.

14.4.1 Genauer gesagt: Sind bei einem polyalphabetischen Verfahren das Referenzalphabet oder die unabhängigen Alphabete, somit auch die Chiffrierschritte und die Dechiffrierschritte bekannt und ist auch bekannt, welche Schlüsselzeichen diese Alphabete kennzeichnen, so kann exhaustiv die partielle Dechiffrierung versucht werden – dabei braucht die Chiffrierung gar nicht periodisch zu sein. Als Beispiele mögen monographische oder polygraphische lineare Substitutionen dienen, bei denen das Referenzalphabet bekannt ist. Diese Möglichkeit wurde schon 1846 von *Charles Babbage* für VIGENÈRE- und BEAUFORT-Chiffrierungen studiert. Auch ALBERTI-Chiffrierungen und PORTA-Chiffrierungen mit bekanntem Referenzalphabet sind diesem Angriff ausgesetzt.

Beispielsweise sei von dem Geheimtext

B A WI S ME WO O P G V R S F I B B T J T WL H WWA H T MJ V B T Z R R E

bekannt, daß er über $\mathbb{Z}_{26}$ mit VIGENÈRE-Schritten ($c_j = p_j + k_j$) chiffriert ist und daß als Alphabet das Standardalphabet dient, ferner daß die Sprache vermutlich Englisch ist. Als wahrscheinliches Wort im Schlüssel könnte man dann jedenfalls *THE* erwarten. Dechiffrierung damit ($p_j = c_j - k_j$) ergibt, wenn man ganz links beginnt, der Reihe nach die Klartextbruchstücke

^{1}/its/, ^{2}/hpe/, ^{3}/dbo/, ^{4}/pli/, ^{5}/zfa/, ^{6}/txs/, ^{7}/lpk/, ^{8}/dhk/, ^{9}/vhl/, ^{10}/vic/, ^{11}/wzr/, ^{12}/non/, ^{13}/cko/, ^{14}/ylb/, ^{15}/zye/, ^{16}/mbx/, ^{17}/pux/, ^{18}/iup/ ... .

Offensichtlich können mit einem so kurzen Wort nicht sehr viele Lagen ausgeschlossen werden; die erste, zweite, dritte, vierte, siebte usw. (durch Unterstreichen markiert) könnten passen. Als nächstes möchte man vielleicht das Wort *THAT* versuchen, das siebthäufigste im Englischen. Damit erhält man nacheinander die Klartextfragmente

^{1}/itwp/, ^{2}/hpiz/, ^{3}/dbst/, ^{4}/plml/, ^{5}/zfed/, ^{6}/txwv/, ^{7}/lpov/, ^{8}/dhow/, ^{9}/vhpn/, ^{10}/vigc/, ^{11}/wzvy/, ^{12}/norz/, ^{13}/cksm/, ^{14}/ylfp/, ^{15}/zyii/, ^{16}/mbbi/, ^{17}/puba/, ^{18}/iutq/, ... ^{27}/dtha/, ^{28}/hatt/ ... ;

von diesen sind nur wenige (unterstrichene) akzeptabel.

Auch dieses Verfahren kann mit Alphabetstreifen mechanisiert werden.

14.4.2 Das Verfahren kann auch umgekehrt durchgeführt werden, wenn Geheimtextzeichen und Klartextzeichen das Schlüsselzeichen eindeutig bestimmen, wenn es sich also um eine Shannonsche Chiffrierung handelt. Dies ist etwa bei linearen Substitutionen mit bekanntem Referenzalphabet ebenfalls der Fall. Im obigen Beispiel könnte als nicht zu kurzes wahrscheinliches Wort im Klartext /should/ dienen. Dies würde ($k_i = c_i - p_i$) der Reihe nach

^{1}*JTIOHJ*, ^{2}*IPUYBB*, ^{3}*EBESTT*, ^{4}*QLYKLL*, ...

ergeben, wobei von den ersten vier Positionen wieder drei ausgeschlossen werden können.

14.4.3 Weder das eine (14.4.1) noch das andere Vorgehen (14.4.2) geben für sich allein viel her. Beide Möglichkeiten können aber in einem **Zick-Zack-Wechselspiel** (engl. *cross-ruff*) kombiniert werden zu einer leistungsfähigen Methode, die *Friedman* 1918 angab.

In unserem Beispiel sei in der achten Position ^{8}/dhow/ , das Gegenstück zu ^{8}*THAT* , herausgegriffen. Man könnte vermuten, daß es verlängert werden kann zu ^{8}/dhowever/. Dies führt auf der Seite des Schlüssels zu der Verlängerung ^{8}*THATCANB* . Des weiteren hat ^{3}/should/ in der dritten Position eine einbuchstabige Überlappung mit ^{8}/dhow/, zusammengenommen ergibt sich ^{3}/shouldhowever/ und als Gegenstück ^{3}*EBESTTHATCANB* . ^{1}*THE* in der ersten Position hat als Gegenstück ^{1}/its/, das überlappt sich und ergibt die Verlängerungen ^{1}/itshouldhowever/ und ^{1}*THEBESTTHATCANB* . Letzteres läßt an ^{1}*THEBESTTHATCANBE* denken, dessen Gegenstück ^{1}/itshouldhoweverb/ zu ^{1}/itshouldhoweverbe/ ergänzt werden kann.

Das Methodische in diesem Vorgehen liegt wieder in der Schaffung von Keimen, die zu Inseln erweitert werden und schließlich zusammenfließen. Das Auftreten von ^{27}/dtha/ als weiteres Gegenstück zu ^{27}*THAT* reizt dazu, die Verlängerung zu ^{27}/dthat/ zu untersuchen, mit dem Gegenstück ^{27}*THATT* ; dies verlängert zu ^{27}*THATTHE* führt zurück zu ^{27}/dthatcr/ und der, zugegebenermaßen kühne Versuch einer Fortsetzung mit ^{27}/dthatcrypt/ hat Erfolg, er führt zu ^{27}*THATTHEDEG* – was wiederum ^{27}*THATTHEDEGREE* nahelegt und als Gegenstück ^{27}/dthatcryptana/ .

Auf diese Weise fortgesetzt, ergibt sich die vollständige Entzifferung (vgl. die Zitate in der Einleitung zum Teil II)

i t s h o u l d h o w e v e r b e e m p h a s i z e d t h a t c r y p t a n a
T H E B E S T T H A T C A N B E E X P E C T E D I S T H A T T H E D E G R E E

Es ist also gefährlich, einen Schlüsseltext in einer gebräuchlichen Sprache zu benützen. Nichtperiodischer Schlüssel verhindert die Zick-Zack-Exhaustion nicht; es kommt nur darauf an, daß sowohl der Schlüsseltext wie auch der Klartext deutlich mehr als 50% Redundanz hat.

14.5 Isomorphie-Methode

ROTOR-Chiffrierungen leiden unter dem Defekt, daß ihre Alphabete kein lateinisches Quadrat bilden müssen. Dadurch wird ein Angriffsweg eröffnet.

14.5.1 Dies zeigt sich besonders bei der **Isomorphie-Methode**, die schon 1935 von *Alfred Dillwyn Knox* (1885–1943) bei einem Bruch der italienischen kommerziellen ENIGMA und 1937 gegen Franco in Spanien benutzt wurde, aber in der offenen Literatur erst 1946 von *Rosario Candela* beschrieben wurde.

Die Isomorphie-Methode wurde für den Fall der kommerziellen ENIGMA als ≪*méthode des bâtons*≫, '*cliques on the rods*' oder '*rodding*' bezeichnet; sie war der Hauptgrund für die Einführung des Steckerbrettes bei der

Wehrmachts-ENIGMA. Im spanischen Bürgerkrieg von 1938–1939 wurden kommerzielle ENIGMAs von allen Seiten – Briten, Deutsche, Italiener, spanische Republikaner – eingesetzt, bei der italienischen Kriegsmarine noch 1941; entsprechend wurde allseits die Isomorphie-Methode benutzt.

Die polyalphabetische Substitution sei von der Form (p_i Klartextzeichen, c_i Geheimtextzeichen)

$$c_i = p_i\ S_i\ U\ S_i^{-1}$$

mit bekannten Alphabeten S_i, deren Reihenfolge ebenfalls bekannt ist – der unbekannte Schlüssel besteht aus dem Anfangsindex der Folge und allenfalls aus U . Bildet man nun die isomorphen (vgl. 2.6.3) Folgen $c_i S_i$ und $p_i S_i$, so gilt

$$c_i S_i = p_i S_i \cdot U\ ;$$

die Folge $(c_i S_i)$ ist also monoalphabetisches Bild der Folge $(p_i S_i)$ unter der Substitution U , die damit durch eine vollständige Klartext-Geheimtext-Kompromittierung genügend langer Texte aufgedeckt ist.

Zwei beliebige Folgen sind im allgemeinen selbstverständlich nicht isomorph: Die Folgen (a l l e . . .) und (g a n g . . .) sind nicht isomorph, weil die Paare (l,a) und (l,n) , wie auch die Paare (a,g) und (e,g) widersprüchlich sind („kreischen“, engl. *screech, scritch*).

Zur Kryptanalyse kommt es also nur darauf an, für ein gegebenes wahrscheinliches Wort einen passenden Anfangsindex i zu finden derart, daß für das $(p_i, p_{i+1}, \ldots p_{i+k})$ lautende Wort $(p_i S_i, p_{i+1} S_{i+1}, \ldots p_{i+k} S_{i+k},)$ und $(c_i S_i, c_{i+1} S_{i+1}, \ldots c_{i+k} S_{i+k},)$ isomorph sind. Widersprüche führen zur Ausschließung des Indexes. Unter den passenden Indizes ist sicher auch der richtige, wenn das wahrscheinliche Wort phasenrichtig zum Geheimtext steht; je länger das wahrscheinliche Wort ist, umso weniger wird man mit Fehltreffern rechnen müssen. Exhaustiv muß im übrigen die Phasenlage des wahrscheinlichen Worts bestimmt werden.

Die obige Voraussetzung liegt insbesondere vor im Fall der rotierten Standardalphabete (7.2.2) mit $\{\ \rho^{-i} R \rho^{i}\ :\ i \in \mathbb{N}\ \}$. Spezifisch hat man diese Situation bei den kommerziellen Maschinen ohne Steckerbrett ENIGMA C und ENIGMA D, mit 3 Rotoren und einer festen oder beweglichen Umkehrwalze (vgl. 7.3.2) mit

$$S_{(i_1,i_2,i_3)} = \rho^{-i_1}\, R_N\, \rho^{i_1-i_2}\, R_M\, \rho^{i_2-i_3}\, R_L\, \rho^{i_3} \quad \text{bzw.}$$
$$S_{(i_1,i_2,i_3,i_4)} = \rho^{-i_1}\, R_N\, \rho^{i_1-i_2}\, R_M\, \rho^{i_2-i_3}\, R_L\, \rho^{i_3-i_4} \quad ,$$

wenn erst einmal alle verwendeten Rotoren aufgeklärt sind – wie es bei einer kommerziellen Maschine ohnehin der Fall war – und ihre Lage bekannt ist (schlimmstenfalls sind bei einer 3-Rotor-ENIGMA sechs Walzenlagen durchzuspielen). Überdies ist in diesem Fall die Isomorphie nun auf involutorisches U beschränkt, es ergeben sich also weitere Möglichkeiten des „Kreischens“ und damit der Ausschließung einer Rotorstellung wie auch die positive Bestätigung einer passenden Rotorstellung durch Auftreten einer

Involution. Die Möglichkeit von Fehltreffern wird dadurch verringert; der involutorische Charakter erleichtert die unbefugte Entzifferung.

Dank der Regelmäßigkeit der Fortschaltung der Rotoren bei der ENIGMA (vgl. 8.5.3) ist es im allgemeinen unnötig, alle 26^3=17 576 bzw. 26^4=456 976 Rotoralphabete durchzuprobieren. Es genügt in der Regel, nur die 26 Stellungen des „schnellen" Rotors R_N zu betrachten, die zwischen zwei Schritten des „mittleren" Rotors R_M liegen. Die beiden anderen Rotoren bleiben solange fest und bilden zusammen mit U eine Pseudo-Umkehrwalze

$$U'_{(i_2,i_3)} = \rho^{-i_2} R_M \rho^{i_2-i_3} R_L \rho^{i_3} \cdot U \cdot \rho^{-i_3} R_M \rho^{i_3-i_2} R_L \rho^{i_2} \quad \text{bzw.}$$

$$U'_{(i_2,i_3,i_4)} = \rho^{-i_2} R_M \rho^{i_2-i_3} R_L \rho^{i_3-i_4} \cdot U \cdot \rho^{i_4-i_3} R_M \rho^{i_3-i_2} R_L \rho^{i_2} ;$$

mit $S_i = \rho^{-i} R_N \rho^i$ hat man $c_i S_i = p_i S_i \cdot U'_{(i_2,i_3)}$ bzw. $c_i S_i = p_i S_i \cdot U'_{(i_2,i_3,i_4)}$.

14.5.2 Für die praktische Durchführung der Isomorphie-Methode gibt es wieder ein Streifen-Verfahren, bei dem als Streifen die einzelnen Spalten der rotierten Alphabete benutzt werden. Nach einem Beispiel von *Deavours* und *Kruh* sei folgende Kompromittierung zu untersuchen

r e c o n n a i s s a n c e
U P Y T E J O J Z E G B O T

Versuchsweise soll der Rotor I der Wehrmachts-ENIGMA benutzt werden. Die Spalten der zu den einzelnen Klartextbuchstaben gehörigen, durch die Rotorstellung bestimmten Chiffren sind in 7.3.5 zu finden. Klartextfragment und Geheimtextfragment werden mit den Streifen gebildet. Die Gegenüberstellung zeigt Abb. 100 . In jeder Zeile, mit Ausnahme der mit der Rotorstellung $i = 2$ bezeichneten, ergeben sich Widersprüche (jeweils einer ist durch Fettdruck hervorgehoben). In der zu $i = 0$ gehörigen Zeile beispielsweise verletzen die Paare A Q und H Q wie auch B N und D N die Injektivität, des weiteren R Y und R D die Eindeutigkeit der Chiffrierung, ferner verstoßen U A und A Q , wie auch F W und W I , Q R und R D , aber auch X U und U A , A Q und Q R, B N und N G , D N und N G , H Q und Q R gegen die involutorische Eigenschaft. In der zu $i = 2$ gehörigen Zeile dagegen finden sich die Zweierzyklen (J U), (M C), (S E) und die Bedingung der Involution ist nicht verletzt; dieser einzige Treffer (engl. *hit*) ergibt folgendes isomorphe Paar von Klartext und Geheimtext

j g m g f u h r w c n s e w
U Z C Z B J O T A M Q E S A

Damit ist der Rotor I als „schneller" Rotor R_N nachgewiesen. Überdies ergeben sich aus den vierzehn Zeichenpaaren bereits neun Zweierzyklen der Pseudo-Umkehrwalze $U'_{(i_2,i_3)}$ bzw. $U'_{(i_2,i_3,i_4)}$, nämlich (A W) , (B F , (C M) , (E S) , (G Z) , (H O) , (J U) , (N Q) , (R T) . Die Methode verlangt also keine langen wahrscheinlichen Wörter.

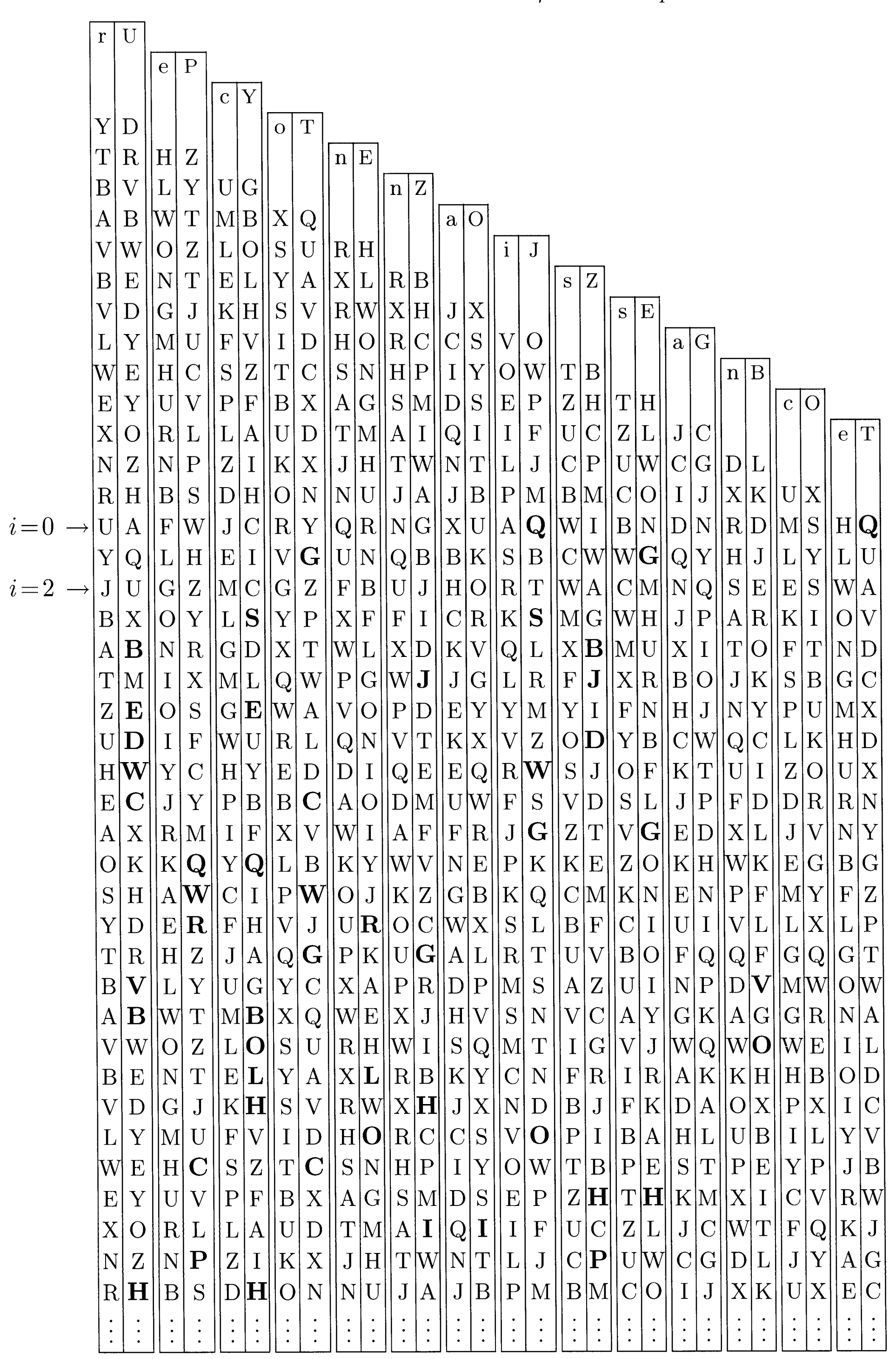


Abb. 100. Isomorphie-Methode mit Streifen (*méthode des bâtons*)

Aus einem vorgefertigten Katalog mit $2 \times 26^2 = 1\,352$ Einträgen aller $U'_{(i_2,i_3)}$ bzw. $2 \times 26^3 = 35152$ Einträgen aller $U'_{(i_2,i_3,i_4)}$ kann dann die Lage und Stellung der beiden für R_M und R_L dienenden Rotoren II und III bestimmt werden. Mit der so gewonnenen Anfangsstellung ist die Entzifferung auf einer ENIGMA oder einem ENIGMA-Nachbau durchführbar. Man geht also von zwei Seiten her vor ('*meet in the middle*'). Die Schweiz benützte, wie auch andere kleine Nationen, während (und teilweise auch nach) dem 2. Weltkrieg ENIGMAs ohne Steckerbrett (mit abgeänderten Rotoren), U.S. Deckname INDIGO. Die Deutschen lasen regelmäßig mit Hilfe von Katalogen gut mit.

14.5.3 Die vorstehenden Überlegungen standen unter der Annahme, daß der „mittlere“ Rotor R_M, entsprechend der Kürze des wahrscheinlichen Worts, während der Chiffrierung sich nicht bewegt. Geschieht dies jedoch, so ändert sich an einer Bruchstelle des Textes die Pseudo-Umkehrwalze, die Untersuchung zerfällt in zwei Teiluntersuchungen, ohne dadurch wesentlich schwieriger zu werden. Es besteht sogar der Vorteil, daß bei der Wehrmachts-ENIGMA die Lage der Nut und damit die Ringstellung aufgedeckt wird (bei der kommerziellen ENIGMA war die Nut fest mit dem Rotor verbunden, für jeden Rotor war die Lage der Bruchstelle bekannt). Hat man vor und nach der Bruchstelle je zwei isomorphe Texte (c', p') und (c'', p''), so kennt man einige Zweierzyklen der Pseudo-Umkehrwalze $U^{(1)}$, die vor der Bruchstelle gilt und $U^{(2)}$, die nach der Bruchstelle gilt. Daraus kann man Lage und Stellung des mittleren Rotors R_M gewinnen. Für eine ENIGMA D verringert sich dadurch der Umfang des weiterhin erforderlichen Katalogs auf $2 \times 26^2 = 1352$ Einträge.

Ein Beispiel (*Deavours*) mag dies illustrieren: Es sei folgende Kompromittierung zu untersuchen

g e n e r a l f e l d m a r s c h a l l k e s s e l r i n g
L S H X B T F W U I O V B C A R X S N C V Z Y X N J B F W B

Es sei angenommen, daß die Untersuchung des Teilworts g e n e r a l bei den Stellungen $i = 17$ bis $i = 23$ einen Treffer ergeben hat und zwei isomorphe Texte. Fortführung bis zu $i = 26$ bestätigt das und liefert

e x o v l y l x r u
M R H F D T D R X G

also die Zweierzyklen (E M), (R X), (H O), (F V), (D L), (T Y), (G U) als Bestandteile von $U^{(1)}$. Der restliche Text muß sich mit $i = 1$ bis $i = 10$ anschließen, er liefert tatsächlich zwei isomorphe Texte

b d a q r w r l j b s p f q c h m o o z
N R W X D A D J L N M Y H X I F S E E T

und die Zweierzyklen (B N), (D R), (A W), (P X), (J L), (S M), (P Y), (F H), (Q X), (C I), (E O), (T Z) als Bestandteile von $U^{(2)}$. Beiden Mengen gemeinsam sind die elf Zeichen D, E, F, H, L, M, O, R, T, X, Y.

Für den als mittlerer Rotor in Frage kommenden Rotor lautet die Tafel der rotierten P-Alphabete:

i	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	L	W	F	T	B	A	X	J	D	S	C	K	P	R	Z	Q	Y	O	E	H	U	G	M	I	V	N
1	O	M	X	G	U	C	B	Y	K	E	T	D	L	Q	S	A	R	Z	P	F	I	V	H	N	J	W
2	X	P	N	Y	H	V	D	C	Z	L	F	U	E	M	R	T	B	S	A	Q	G	J	W	I	O	K
3	L	Y	Q	O	Z	I	W	E	D	A	M	G	V	F	N	S	U	C	T	B	R	H	K	X	J	P
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Für die gemeinsamen elf Zeichen D, E, F, H, L, M, O, R, T, X, Y hat man nun folgende Tafel der $U^{(1)}$- und $U^{(2)}$-Bilder:

$U^{(1)}$:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
i				l	m	v		o				d	e		h			x		y				r	t	
0				K	P	G		Z				T	B		J			I		V				O	H	
1				D	L	V		S				G	U		Y			N		J				Z	F	
2				U	E	J		R				Y	H		C			I		O				S	Q	
3				G	V	H		N				O	Z		E			X		J				C	B	
⋮				⋮	⋮	⋮		⋮				⋮	⋮		⋮			⋮		⋮				⋮	⋮	

$U^{(2)}$:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
i				r	o	h		f				j	s		e			d		z				q	p	
0				O	Z	J		A				S	E		B			T		N				Y	Q	
1				Z	S	Y		C				E	P		U			G		W				R	A	
2				S	R	C		V				L	A		H			Y		K				B	T	
3				C	N	E		I				A	T		Z			O		P				U	S	
⋮				⋮	⋮	⋮		⋮				⋮	⋮		⋮			⋮		⋮				⋮	⋮	

Betrachtet man jetzt $i=0$ von $U^{(1)}$ und $i=1$ von $U^{(2)}$, so findet man den Buchstaben Z in der Zeile $i=0$ unter h, in der Zeile $i=1$ unter d:

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0				K	P	G		**Z**				T	B		J			I		V				O	H	
1				**Z**	S	Y		C				E	P		U			G		W				R	A	

In dem entsprechenden Ausschnitt aus der Tafel der rotierten P-Alphabete

i	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	L	W	F	T	B	A	X	**J**	D	S	C	K	P	R	Z	Q	Y	O	E	H	U	G	M	I	V	N
1	O	M	X	**G**	U	C	B	Y	K	E	T	D	L	Q	S	A	R	Z	P	F	I	V	H	N	J	W

findet sich jedoch keine entsprechende Übereinstimmung. Diese Rotorstellung „kreischt“ also.

Betrachtet man dagegen $i=1$ von $U^{(1)}$ und $i=2$ von $U^{(2)}$, so findet man

den Buchstaben L in der Zeile $i=1$ unter e, in der Zeile $i=2$ unter l,
den Buchstaben V in der Zeile $i=1$ unter f, in der Zeile $i=2$ unter h,
den Buchstaben S in der Zeile $i=1$ unter h, in der Zeile $i=2$ unter d,
den Buchstaben Y in der Zeile $i=1$ unter o, in der Zeile $i=2$ unter r:

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1				D	**L**	**V**		**S**				G	U		**Y**			N		J				Z	F	
2				**S**	R	C		**V**				**L**	A		H			**Y**		K				B	T	

In dem entsprechenden Ausschnitt aus der Tafel der rotierten *P*-Alphabete

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	O	M	X	G	**U**	**C**	B	**Y**	K	E	T	D	L	Q	**S**	A	R	Z	P	F	I	V	H	N	J	W
2	X	P	N	**Y**	H	V	D	**C**	Z	L	F	**U**	E	M	R	T	B	**S**	A	Q	G	J	W	I	O	K

herrscht in allen Fällen entsprechende Übereinstimmung (mit **Y** für **S**, **U** für **L**, **C** für **V**, **S** für **Y**). Man hat einen Treffer, die richtige Stellung des mittleren Rotors ist somit gefunden.

Auch diese Bestimmung der Rotorstellung läßt sich durch Streifen mit den einzelnen Spalten der rotierten Alphabete praktisch durchführen.

14.5.4 Eine Variante der Methode dient zur Bestimmung der Zweierzyklen der Umkehrwalze U. Dies war in *Bletchley Park* notwendig, seit die Deutschen ab 1944 in der Wehrmachts-ENIGMA gelegentlich eine Umkehrwalze mit schaltbarer Verdrahtung einsetzten (7.3.3). Nunmehr muß für alle 26^3=17 576 Anfangsstellungen die Isomorphieuntersuchung mit einem geeigneten wahrscheinlichen Spruchanfang durchgeführt werden. Dies erfordert spezielle Maschinen, etwa die in den U.S.A. von der *F Branch* der *Army Signal Security Agency* unter dem Kommando von *Colonel Leo Rosen* gebauten AUTOSCRITCHER (Relaismaschine, ab 1944) und SUPERSCRITCHER (elektronisch, ab 1946).[1] [2]

14.5.5 Das Steckerbrett läßt die geschilderte Isomorphie-Methode zusammenbrechen, weil die unbekannte Steckerverbindung das wahrscheinliche Klartextwort verschleiert. Nunmehr ist man darauf angewiesen — dies erfordert allerdings längere Texte — wiederholt auftretende Paare von Klartext- und korrespondierendem Geheimtextzeichen zu suchen. Jede Gruppe solcher Paare geht unter der Steckerverbindung wieder in eine Gruppe gleicher Paare über. Die Isomorphie verlangt, daß die Gruppen beim Durchspielen aller Rotorstellungen nicht auseinanderfallen.

Die Maschinen AUTOSCRITCHER und SUPERSCRITCHER waren auf diese Aufgabe hin ausgelegt. Verwandt waren die britische Maschine GIANT und die Maschine DUENNA der U.S. Navy. Ein ersatzweise manuell durchzuführendes Verfahren ('Hand-Duenna') wurde von C. H. O'D. Alexander 1944 in einem internen Vermerk für Bletchley Park (*Fried Reports*) festgehalten.

---

1 *Scritch* ist eine Dialektvariante von *screech*, kreischen.

2 In der offenen Literatur wird *scritch*, *scritchmus* ohne nähere Erklärung verwendet, so von *Derek Taunt* (1993) bei einer Schilderung der Arbeiten in *Bletchley Park* unter Bezug auf Aufgaben, die *Dennis Babbage* hatte, wobei auch die schaltbare Umkehrwalze erwähnt wird. Bei den Briten wird man also den Ursprung des Terminus zu suchen haben. *David Crawford* und *Philip Fox* (1992) berichten, daß sie über den kryptologischen Hintergrund von AUTOSCRITCHER und SUPERSCRITCHER nicht eingeweiht waren. Aus einer Arbeit von *Cipher Deavours* (1995) ergibt sich der Zusammenhang mit der Isomorphiemethode.

14.6 Verdeckte Klartext-Geheimtext-Kompromittierung

Die Methoden des wahrscheinlichen Wortes sollen den vollen Klartext herstellen helfen. Im Falle einer Klartext-Geheimtext-Kompromittierung ist das gar nicht mehr nötig. In glücklich gelagerten Fällen kann jedoch der Schlüssel gefunden und damit ein tiefer Einbruch in das System erzielt werden. Dazu sind technisch alle bisher besprochenen Mittel des Angriffs mit wahrscheinlichen Wörtern verfügbar; diese können nun überdies komfortabel lang gewählt werden.

Man kann vermuten oder hoffen — je nachdem auf welcher Seite man steht — daß direkte Klartext-Geheimtext-Kompromittierung selten vorkommt. Eine verdeckte Klartext-Geheimtext-Kompromittierung entsteht jedoch, wenn der selbe Klartext zwei verschiedenen Chiffriersystemen unterworfen wurde — eigentlich eine harmlose Geheimtext-Geheimtext-Kompromittierung — und eines der beiden, in der Regel das kryptologisch einfachere, gebrochen wurde. Dann ergibt sich für das schwierige zu brechende System eine Klartext-Geheimtext-Kompromittierung mit allen Konsequenzen.

Es gibt kaum überschaubar viele Arten von Nachlässigkeit und Einfältigkeit, die zu einer solchen Situation führen können. Ein Grund kann darin liegen, daß beim Schlüsselnachschub Probleme auftreten und eine Nachricht, die noch im alten Schlüssel übermittelt wurde, im neuen Schlüssel nochmals gesendet wird. Daß nämlich der alte Schlüssel gebrochen wurde, muß man gegen Ende seiner Laufzeit ohnehin eher erwarten: "*The risk, that a cryptosystem is broken is never greater than at the end of its lifetime*" sagt eine kryptologische Wetterregel. Auf diese Weise wurde nach *Hüttenhain* zwischen 1942 und September 1944 eine Reihe von sogenannten CQ-Funksprüchen ('*call to quarters*') des State Departments in Washington an seine diplomatischen Vertretungen von den Deutschen mitgelesen. Die für CQ-Funksprüche reservierten Lineale der M-138 waren für alle Botschaften identisch. Beim Wechsel der Lineale mußten solche Pannen vorkommen.

Wegen der besonderen Gefahr einer Preisgabe des ganzen Chiffriersystems durch eine Klartext-Geheimtext-Kompromittierung kam *Hüttenhain* retrospektiv zu dem Schluß „Es dürfen also keine Chiffrierverfahren verwendet werden, die gegen Klar-Geheim-Kompromisse anfällig sind". In Verbindung mit *Kerckhoffs*' Maxime bedeutet die *Hüttenhain*sche Maxime, daß viele klassische und etliche moderne Systeme, Vorschriften und Gewohnheiten über Bord geworfen werden müssen. Insbesondere darf kein solches System die Shannon-Eigenschaft (2.6.4) haben.

Fehler wurden überall gemacht. *Kahn* bemerkte dazu "*the Germans had no monopoly on cryptographic failure. In this respect the British were just as illogical as the Germans*".

15 Anatomie der Sprache: Häufigkeit

"We can only say that the decryptment of any cipher even the simplest will at times include a number of wonderings."

Helen Fouché Gaines 1939

Die im 13. Kapitel besprochene Entzifferung mit Hilfe der Mustererkennung benutzt von der Anatomie der Sprache das Skelett. Die nunmehr zu besprechenden Methoden zielen auf die Weichteile: Sie gehen auf statistische Gesetzmäßigkeiten der Sprache, insbesondere auf Häufigkeiten, aus. Erste Ansätze findet man bei dem ostarabischen Philosphen *al-Kindī* (um 800–870), und schon 1466 wußte der italienische '*uomo universale*' *Leone Battista Alberti* (1404–1472) darüber zu berichten (*Trattati in cifra*, 1470). Eine theoretische Erklärung der Stabilität der Zeichenhäufigkeiten in natürlichen Sprachen geht auf *Ferdinand de Saussure* (publ. 1916) zurück.

Zunächst haben wir den offensichtlichen

Invarianzsatz 2: Für alle Transpositionen gilt:
Häufigkeiten der Einzelzeichen innerhalb des Textes bleiben erhalten.

15.1 Ausschließung von Chiffrierverfahren

Satz 2 kann negativ zur Ausschließung von Transpositionen gebraucht werden — wenn nämlich die Häufigkeit der Einzelzeichen des Chiffrats der vermuteten Sprache ganz und gar nicht entspricht.

15.1.1 Die Geheimnachricht

```
FDRJN  UHVXX  URDMD  SKVSO  PJRKZ  DYFZJ
XGSRR  VTQYR  WDARW  DFVRK  VDRKV  TDFSZ
ZDYFR  DNNVO  VTSXS  AWVZR
```

hat als häufigste Zeichen R, D, V, S ; überaus selten, nämlich gar nicht vorhanden sind B, C, I, E . Sie kann kaum aus einem deutschen, englischen, französischen oder italienischen Klartext durch Transposition entstanden sein. (Tatsächlich liegt, vgl. 13.3.1, eine einfache Substitution vor).

15.1.2 Dagegen ist nicht auszuschließen, daß die Geheimnachricht

```
SAEWS  HRCNU  ODKLN  ELIAS  HNCIO  NBNNA
AKIHM  CWNZA  MCGIM  IHEEN  NAUFK  NNCTI
TIHMD  RTEWO  ATAIM  TALKB  UEAFZ  LNUSE
ASDEN  .....
```

(mit E und T unter den häufigsten Einzelzeichen und fehlenden V, P, J, Q, X und Y) durch Transposition eines deutschen Textes entstanden ist (vgl. 12.5, Tabelle 6).

15.1.3 Satz 2 wird auch (logisch unzulässig) verwendet im Sinne des plausiblen Schließens: Ist die Häufigkeitsverteilung der Einzelzeichen die einer in Betracht kommenden natürlichen Sprache, so liegt *vermutlich* Transposition vor. Die naive Argumentation lautet: Was sonst – welches andere Verfahren würde die Häufigkeitsverteilung der Einzelzeichen invariant lassen? Sie ist natürlich falsch: Es kann zwar keine nichttriviale einfache monoalphabetische Substitution vorliegen, aber man kann unschwer eine Polygramm-Substitution, etwa einen Code, konstruieren, derart daß die Einzelzeichenhäufigkeitsverteilung der Geheimnachrichten hinreichend genau mit einer vorgegebenen Einzelzeichenhäufigkeit übereinstimmt (vgl. 4.1.2). *W. B. Homan* hat 1948 ein solches Verfahren angegeben, bei dem alle Geheimtextzeichen gleich häufig auftreten (*'equifrequency cipher'*). Das gleiche wird erreicht durch eine redundanzvermindernde Shannon-Huffman-Codierung.

Mit derartigen Tricks kann man den unbefugten Entzifferer aber nicht allzu lange hinhalten. Immerhin wurde *Bazeries*, als er 1892 eine Nachricht brechen sollte, die einer französischen Anarchistengruppe abgenommen worden war, für 14 Tage aufgehalten, weil er in die falsche Richtung geführt wurde durch je sechs am Anfang und am Ende angefügte und mehrere in den Text als Blender eingestreute seltene Buchstaben. Tatsächlich war die Nachricht lediglich linear polyalphabetisch mit einer Periodenlänge 6 chiffriert. Am Anfang und Ende gerade soviel Zeichen anzufügen, wie die Periodenlänge beträgt, mag ein Fehler gewesen sein, trotzdem war die Irreführung nach *Bazeries* eigenem Bekunden vorzüglich gelungen. Ein Teil der entzifferten tödlichen Nachricht lautete übrigens: *≪La femme et lui sont des mouchards, s'il m'arrive quelque chose, songe à les supprimer.≫*

15.2 Invarianz der Partitionen

Eine **Partition** ist eine Zerlegung einer natürlichen Zahl M in eine Summe von natürlichen Zahlen m_i. Zu jedem (Klar-)Text der Länge M gehört eine Partition von M, nämlich in die Anzahlen, mit denen die einzelnen Zeichen vorkommen. Zum Text w i n t e r s e m e s t e r gehört die Partition $14 = 4+2+2+2+1+1+1+1$. Wir sprechen von einer Einzelzeichen-Partition.

Es gilt der fundamentale, zu 13.1, Satz 1 parallele

> **Invarianzsatz 3:** Für alle monoalphabetischen, funktionalen einfachen Substitutionen, insbesondere auch für alle linearen monoalphabetischen einfachen Substitutionen gilt:
> *Einzelzeichen-Partitionen innerhalb des Textes bleiben erhalten.*

Ein entsprechendes Chiffrat von w i n t e r s e m e s t e r besteht also aus vier Exemplaren eines gewissen Zeichens, zwei Exemplaren eines gewissen anderen Zeichens, zwei Exemplaren eines gewissen dritten Zeichens, und so weiter.

Die Partition 14 = 4+2+2+2+1+1+1+1 ist invariant. Würde der unbefugte Entzifferer die zum Chiffrat

Z L Q W H U V H P H V W H U

gehörige Häufigkeit des Vorkommens der Zeichen im Klartext kennen, also wissen, daß /e/ viermal, /t/ zweimal, /r/ zweimal, /s/ zweimal, /n/ einmal, /i/ einmal, /w/ einmal, /m/ einmal vorkommt, so wüßte er, daß H$\hat{=}$e, {UVW}$\hat{=}${r s t}, {LPQZ}$\hat{=}${i m n w} und hat die polyphone Dechiffrierung

i	i	i	r		r	r		i		r	r		r
m	m	m	s	e	s	s	e	m	e	s	s	e	s
n	n	n	t		t	t		n		t	t		t
w	w	w						w					

Nun folgt aber die Häufigkeit der Einzelzeichen inneren Gesetzen der Sprache. In einfachster Näherung kommt jedem Einzelzeichen χ_i eine Wahrscheinlichkeit p_i des Auftretens (‚stochastische Quelle' Q) zu, derart, daß die Häufigkeit $m_i = Q[\chi_i]$ seines Vorkommens in einem Text der Länge M nahe bei $M \cdot p_i$ liegt.

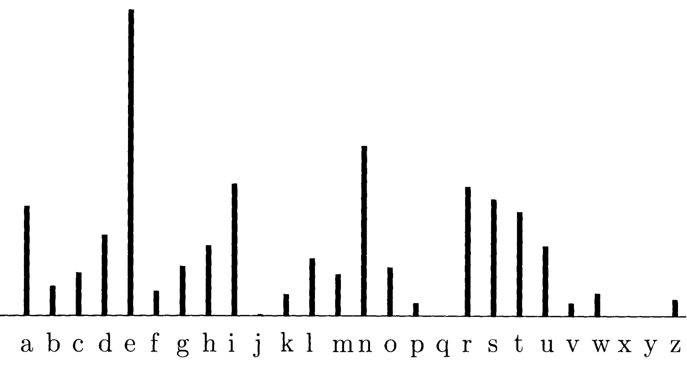


Abb. 101. Häufigkeitsgebirge im Deutschen

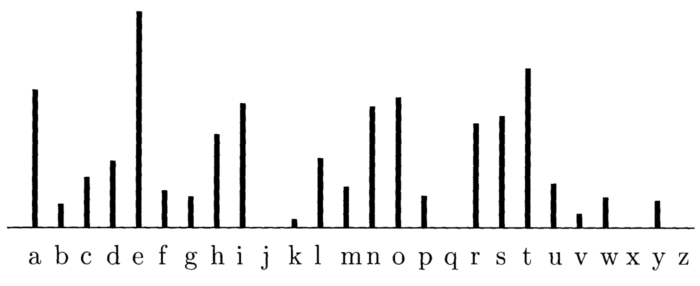


Abb. 102. Häufigkeitsgebirge im Englischen

15.3 Intuitive Häufigkeitserkennung: Häufigkeitsgebirge

Zur intuitiven Häufigkeitserkennung ist es zweckmäßig, sich das ‚Häufigkeitsgebirge' einer Sprache optisch einzuprägen.

Im Deutschen (Abb. 101) sind besonders auffällig die e-Spitze und der n-Gipfel, die f-g-h-i-Flanke mit anschließender j-k-Senke, die o-p-q-Senke mit anschließendem r-s-t-u-Kamm.

Demgegenüber bestehen im Englischen (Abb. 102) signifikante Unterschiede: Es ist ein a-Gipfel ausgeprägter, es besteht ein h-i-Kamm und ein l-m-n-o-Kamm, der r-s-t-u-Kamm hat einen t-Gipfel; jedoch finden sich b-c-d-Flanke, j-k-Senke und v-w-x-y-z-Niederung wieder.

Andere europäische Sprachen zeigen keine Unterschiede, die größer sind als die zwischen Deutsch und Englisch. Romanische Sprachen haben ebenfalls einen ausgeprägteren a-Gipfel, im großen und ganzen sind die Profile ähnlich.

15.3.1 Liegt eine Transposition vor, so ergibt eine Häufigkeitszählung direkt das Häufigkeitsgebirge. Aber auch eine lineare monoalphabetische einfache Substitution mit $q = 1$, eine CAESAR-Addition, springt sofort ins Auge:

> **Invarianzsatz 4:** Für alle CAESAR-Additionen gilt:
> *Das Häufigkeitsgebirge des Textes ist lediglich verschoben, und zwar mit zyklischer Schließung.*

Die Geheimnachricht von 349 Zeichen

H V Z D U	V F K R Q	G X Q N H	O D O V L	F K L Q E	R Q Q D Q
N D P L F	K C Z D Q	J P L F K	P H L Q H	D Q N X Q	I W Q L F
K W P L W	G H U D X	W R P D W	L N D E O	D X I H Q	C X O D V
V H Q G L	H V L F K	L Q I X H	Q I M D H	K U L J H	P X Q W H
U Z H J V	V H L Q K	H U D X V	J H E L O	G H W K D	W E D K Q
V W H L J	W U H S S	H U X Q W	H U E D K	Q V W H L	J W U H S
S H U D X	I U H L V	H W D V F	K H D E V	W H O O H	Q I D K U
N D U W H	D X V G H	U P D Q W	H O W D V	F K H Q H	K P H Q U
H L V H W	D V F K H	D X I Q H	K P H Q I	D K U N D	U W H D E
J H E H Q	C X P C H	L W X Q J	V V W D Q	G D E H Q	G C H L W
X Q J H Q	N D X I H	Q Q D F K	G U D X V	V H Q J H	K H Q X Q
G H L Q W	D A L K H	U D Q Z L	Q N H Q		

hat das in Abb. 103 aufgeführte Häufigkeitsgebirge. Man erkennt mit einem Blick, daß es sich um einen CAESAR mit einer Verschiebung um 3 Zeichen handelt. (Der entzifferte Text, vgl. auch 12.5, Tabelle 5, ist der Anfang eines 1963 erschienenen Romans.)

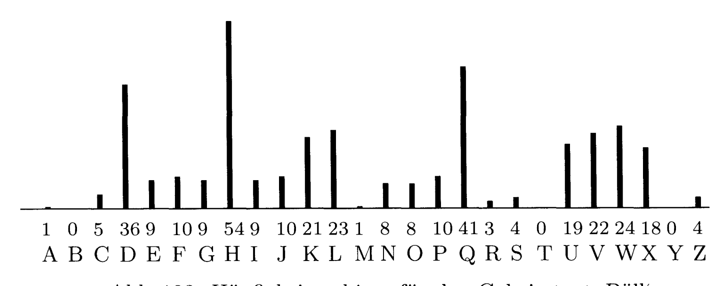


Abb. 103. Häufigkeitsgebirge für den Geheimtext ‚Böll'

15.3.2 Aus dem Auftreten eines verschobenen Häufigkeitsgebirges kann man umgekehrt nicht auf einen CAESAR schließen: Es könnte sich auch um eine Kombination von Transposition und CAESAR-Addition handeln.

15.3.3 Natürlich kann diese Methode auch sonst irreführen, etwa bei folgendem Geheimtext von 175 Zeichen

V Q P O U	I K T C B	N H P K O	H U P T I	P X Z P V	I P X B C
V O D I P	G C S K H	I U Z P V	O H G P M	L T E K E	G K O E B
D I B N Q	K P O B N	B O X K U	I C P Z T	B O E H K	S M T P G
I K T P X	O B N B O	P G T P E	P N K O U	K O H B O	E I B Q Q
Z K O E K	W K E V B	M K U Z U	I B U Z P	V U I K T	E S B X O
U P I K N	B T K T B	G M Z U P	B T V H B	S C P X M	

Das Häufigkeitsgebirge (Abb. 104) zeigt eine große Abweichung von dem der Abb. 101 oder Abb. 102. Es kommt jedoch leicht der Verdacht auf, daß ebenfalls ein CAESAR (über Z_{25}) mit einer Verschiebung um 1 Zeichen vorliegt: '*upon this basis i am going to show .....*' – die Streifenmethode von 12.7 liefert schon für die ersten vier Zeichen so gut wie eindeutig '*upon*'. Daß die Häufigkeitserkennung versagt, liegt daran, daß der Text ein aus "Gadsby" (vgl. 13.3.2, Abb. 88) entnommenes Lipogramm ist.

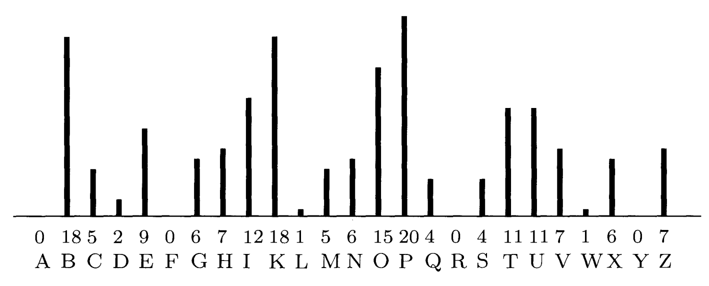


Abb. 104. Häufigkeitsgebirge für den Geheimtext ‚Gadsby' (13.3.2)

15.4 Häufigkeitsreihenfolge

Für eine einfache monoalphabetische Substitution, die nicht linear mit $q = 1$ oder $q = -1$ ist, besagt das Häufigkeitsgebirge nichts mehr – die einzelnen Buchstabennachbarschaften sind zerrissen. Die naive Intuition setzt in diesem Fall an der Häufigkeitsreihenfolge an: Das häufigste Zeichen im Geheimtext sollte dem häufigsten Buchstaben der betreffenden Sprache entsprechen; nach Entfernen des so bestimmten Paares wiederholt sich das Verfahren für den Rest, bis alle Zeichen erschöpft sind.

15.4.1 Theoretisch sollte das Verfahren zumindest für genügend lange Texte zum Ziel führen – genügend lang würde u.a. heißen, daß die wenigen Lipogramme, die es in der Literatur gibt, untergehen gegenüber der Masse der „normalen" Texte. Aber das Beispiel von 15.2, das zu einer polyphonen Situation sogar dann führt, wenn die wahren Häufigkeiten der Klartextzeichen bekannt sind, zeigt die fundamentale Grenze dieses Vorgehens: Wenn Geheimtextzeichen gleicher Häufigkeit vorliegen, ist die Dechiffrierung nichtdeterministisch.

Überdies zeigen sogar lange Texte beträchtliche Fluktuationen der Zeichenhäufigkeiten. Von *der* Häufigkeitsverteilung der englischen Sprache zu sprechen, ist eine Fiktion. Bestenfalls zeigen die Fachsprachen des Militärs, der Diplomatie, des Handels oder der Literatur eine gewisse Homogenität, wobei ein und die selbe Person nach den Umständen eine verschiedene Sprache spricht. Praktisch schwanken dementsprechend die Angaben über die Häufigkeiten der einzelnen Buchstaben in verschiedenen Sprachen sehr. Überwiegend liegen diesen Werten Auszählungen von Texten mit nur 10 000 oder weniger Buchstaben zugrunde. Darauf werden wir in 15.5 zurückkommen.

Schon für die Häufigkeitsreihenfolge findet man verschiedene Angaben, und zwar in jedem Werk andere, die nur in groben Zügen übereinstimmen:[1]

Für die deutsche Sprache:

enrisdutaghlobmfzkcwvjpqxy	(*Ch. Vesin de Romanini* 1840)
enirsahtudlcgmwfbozkpjvqxy	(*F.W. Kasiski* 1863)
enirstudahgolbmfzcwkvpjqxy	(*E.B. Fleissner von Wostrowitz* 1881)
enritsduahlcgozmbwfkvpjqxy	(*P. Valério* 1893)
enrisatdhulcgmobzwfkvpjyqx	(*F. W. Kaeding* 1898)
enritsduahlcgozmbwfkvpjyqx	(*M. Givierge* 1925)
enirstudahgolbmfczwkvpjqxy	(*A. Figl* 1926)
enirsadtugholbmcfwzkvpjyqx	(*H.F. Gaines, J. Arthold* 1939)
enristudahglocmbzfwkvpjqxy	(*L. D. Smith* 1943)
enritsudahlcgozmbwfkvpjqxy	(*L. Sacco* 1951)
enisrtahduglcofmbwkzvpjyqx	(*Ch. Eyraud* 1953)
enristdhaulcgmobzwfkvüpäöjyqx	(*K. Küpfmüller, H. Zemanek* 1954)
enisratduhglcmwobfzkvpjqxy	(*W. Jensen* 1955)
enirsatdhulgocmbfwkzpvjyxq	(*F. L. Bauer* 1993)

Für die englische Sprache:

etaoinshrdlucmfwypvbgkqjxz	(*O. Mergenthaler* 1884)
etoanirshdlcfumpywgbvkxjqz	(*P. Valério* 1893)
etaoinsrhlducfmwygpbvkxjqz	(*G. Dewey* 1923)
etaonisrhldcupfmwybgvkqxjz	(*H.F. Gaines, O.P. Meaker* 1939)
etoanirshdlcwumfygpbvkxqjz	(*L. D. Smith* 1943)
etoanirshdlufcmpywgbvkxzjq	(*L. Sacco* 1951)
etaonirshdlucmpfywgbvjkqxz	(*D. Kahn* 1967)
etaonrishdlfcmugpywbvkxjqz	(*A.G. Konheim* 1981)

Für die französische Sprache:

eusranilotdpmcbvghxqfjyzkw	(*Ch. Vesin de Romanini* 1840)
ensautorilcdvpmqfgbhxyjzkx	(*F.W. Kasiski* 1863)

[1] Die Auszählung von *K. Küpfmüller* und *H. Zemanek*, die die deutschen Umlaute berücksichtigt, ist natürlich kryptologisch uninteressant; sie ist lediglich zu Vergleichszwecken aufgeführt.

esriantouldmcpvfqgxjbhzykw	(*A. Kerckhoffs* 1883)
easintrulodcpmvqfgbhjxyzkw	(*G. de Viaris* 1893)
enairstuoldcmpvfbgqhxjyzkw	(*P. Valério* 1893, *M. Givierge* 1925)
eaistnrulodmpcvqgbfjhzxykw	(*H.F. Gaines* 1939)
etainroshdlcfumgpwbyvkqxjz	(*Ch. Eyraud* 1953)

Angaben für italienisch, spanisch, holländisch, lateinisch finden sich bei *Lange-Soudart 1935.*

Für die ersten rund ein Dutzend Buchstaben gibt es hübsche Merksprüche, etwa

deutsch:	enirstaduhl	(*Hüttenhain*)
englisch:	etaoinshrdlu	(LINOTYPE)
französisch:	esarintulo	(*Bazeries, Givierge*)
italienisch:	eiaorlnts	(*Sacco*) .

Die Häufigkeitsverteilung im Englischen spiegelt sich bereits in der Länge der Morsezeichen wieder – *Morse* hatte den Setzkasten einer Druckerei in Philadelphia ausgezählt und gefunden: 12 000 /e/, 9 000 /t/, je 8 000 /a/, /i/, /n/, /o/, /s/, 6 400 /h/. Die Häufigkeitsverteilung bestimmte aus technischen Gründen auch die Anordnung (etaoin – shrdlu – cmfwyp – ...) auf der Tastatur (Abb. 105) der Zeilensetzmaschine LINOTYPE , die 1884 von *Ottmar Mergenthaler* (1854–1899) erfunden wurde.

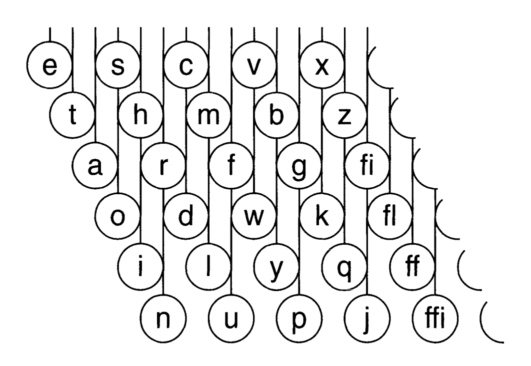


Abb. 105. Originaltastatur von *Ottmar Mergenthaler*

15.4.2 Für die deutsche Sprache hat *F. W. Kaeding* 1898 eine sehr umfangreiche Häufigkeitszählung vorgenommen; er untersuchte für Zwecke der Stenographie Texte, die zusammen 20 Millionen Silben umfaßten und kam damit (Umlaute ä, ö, ü durch ae, oe, ue ersetzt) auf 62 069 452 Buchstaben. Man kann annehmen, daß diese Auszählung ziemlich zuverlässig ist.

Nimmt man die darauf basierende Reihenfolge, wie sie oben angegeben ist, und stellt sie der Reihenfolge der Häufigkeiten im Text ‚Böll' (Abb. 103) gegenüber, so ergäbe sich (bei alphabetischer Reihenfolge der gleichhäufigen Chiffren) die Dechiffriertabelle

54	41	36	24	23	22	21	19	18	10	10	10	9	9	9	8	8	5	4	4	3	1	1	0	0	0
H	Q	D	W	L	V	K	U	X	F	J	P	E	G	I	N	O	C	S	Z	R	A	M	B	T	Y
e	n	r	i	s	a	t	d	h	u	l	c	g	m	o	b	z	w	f	k	v	p	j	y	q	x .

Beginnt man damit den Anfang des Geheimtexts von 15.3.1

HVZDU VFKRQ GXQNH ODOVL FKLQE RQQDQ

zu dechiffrieren, so erhält man

e a k r d a u t v n m h n b e z r z a i u t i n g v n n r n ,

einen völlig inakzeptablen Klartext. Nimmt man die gleichhäufigen Chiffren in anderer Reihenfolge, wird es nicht besser. Aber auch die anderen Häufigkeitsreihenfolgen bringen nichts. Tatsächlich lautet die Dechiffriertabelle, die (vgl. 15.3.1) auf Rückwärtszählen um drei Buchstaben hinausläuft

H	Q	D	W	L	V	K	U	X	F	J	P	G	E	I	O	N	C	Z	S	R	A	M	Y	B	T
e	n	a	t	i	s	h	r	u	c	g	m	d	b	f	l	k	z	w	p	o	x	j	v	y	q .

und gibt folgende Entzifferung

e s w a r s c h o n d u n k e l a l s i c h i n b o n n a n .

15.5 Cliquen und Partitionsanpassung

Abb. 106 zeigt, daß sich die wirklich auftretende Häufigkeitsreihenfolge von der theoretisch zu erwartenden ganz beträchtlich unterscheidet. Es ergeben sich lokale Permutationen, wobei /r/ und /v/ um fünf Plätze springen, /d/, /l/ und /o/ sogar um sechs. Andere Buchstaben springen nur um ein oder zwei Plätze, aber nur wenige – darunter /e/, /n/ – stehen sich gegenüber. Sicher beruhen diese Schwankungen auf der kurzen Länge von 239 Zeichen des Textes, wodurch die wirklich auftretenden Häufigkeiten innerhalb von Bereichen schwanken, die sich sogar überlappen und dadurch zu Überkreuzungen führen; aber, wie sich zeigen wird, verschwinden die Schwankungen auch bei langen Texten nicht völlig. Die bloße Häufigkeitsreihenfolge bringt im allgemeinen keine automatische Entzifferung.

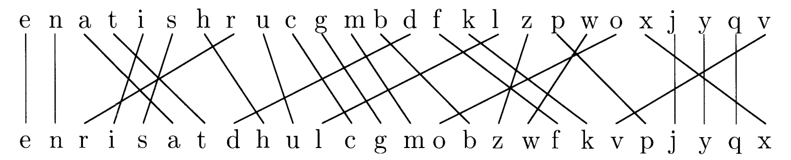


Abb. 106. Gegenüberstellung beobachteter und auf der Wahrscheinlichkeit beruhender Häufigkeitsreihenfolge für den Geheimtext ‚Böll‘ von 15.3.1

In der Tat schwanken in der Literatur nicht nur die Angaben über die Häufigkeitsreihenfolge, sondern auch über die Häufigkeiten selbst, hervorgerufen auch durch das Genre der Texte, über die sich die Auszählung erstreckt. Statt die einzelnen *ad hoc* Auszählungen wiederzugeben, die sich in der Literatur finden, wird es also besser sein, die Bereiche anzugeben, in denen die empirischen Häufigkeiten bei Texten von 1 000 Zeichen, von 10 000 Zeichen oder von 100 000 Zeichen schwanken. Dies wird dazu führen, Teilmengen von

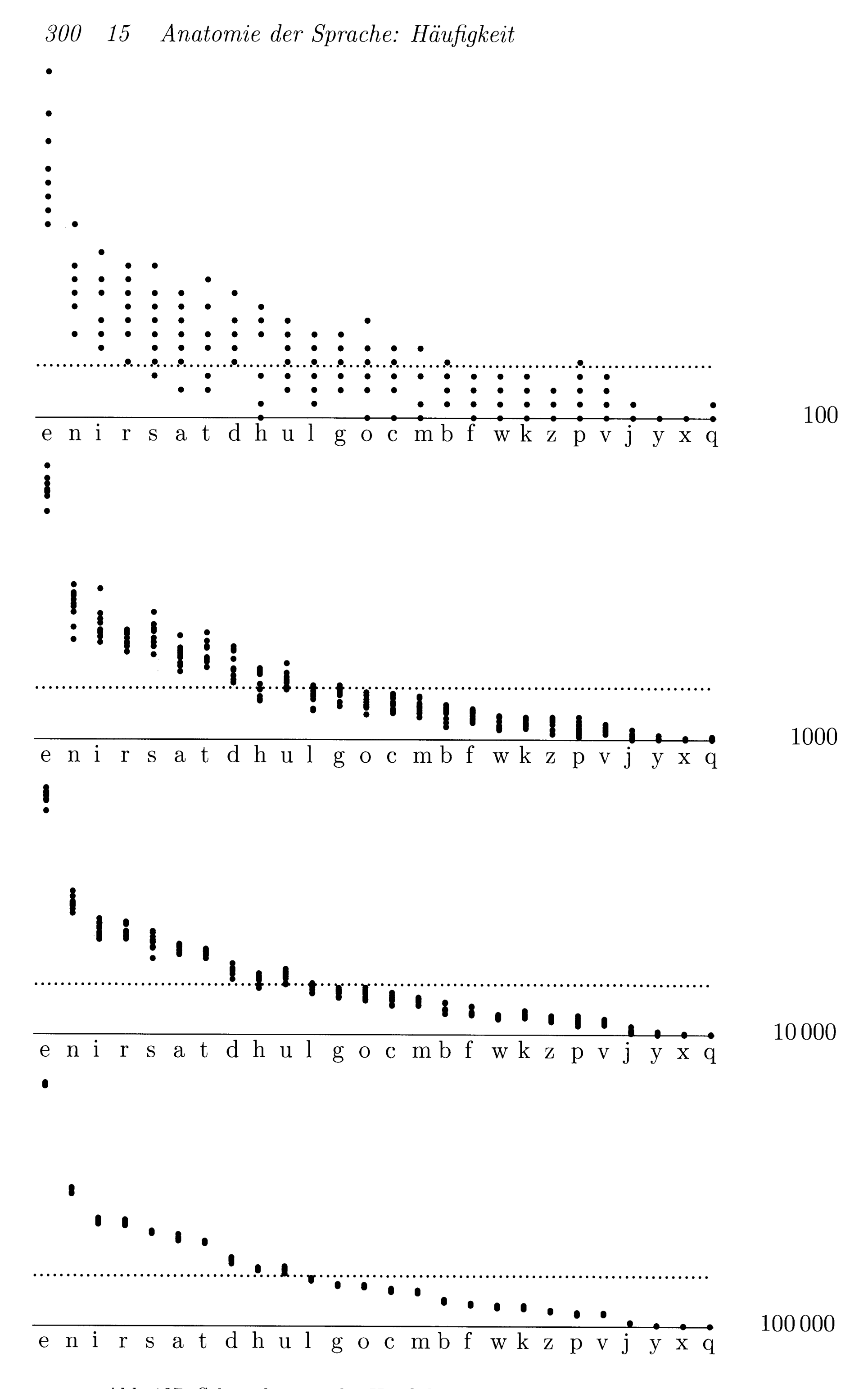


Abb. 107. Schwankungen der Häufigkeiten der Einzelzeichen im Deutschen

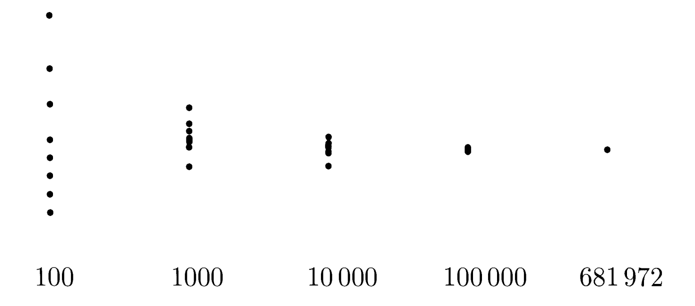


Abb. 108. Schwankungen der Häufigkeiten des /e/ im Deutschen abhängig von der Länge des Textes

Zeichen (‚Cliquen') einzuführen, die sich bei gegebenem Umfang des Textes häufigkeitsmäßig nicht unterscheiden lassen.

15.5.1 Das Ergebnis einer umfangreichen Untersuchung, bei der jeweils 10 Fälle von Texten mit $M = 100$ Zeichen, $M = 1\,000$ Zeichen, $M = 10\,000$ Zeichen oder $M = 100\,000$ Zeichen analysiert wurden, findet sich für die deutsche Sprache in Abb. 107 (gestrichelt: durchschnittliche Häufigkeit). Als Textbasis dienten politische Kommentare, nämlich die gesammelte 'Seite Drei' der Süddeutschen Zeitung vom März 1992 (hinfort Textbasis *SZ3-92* genannt). Es zeigt sich, daß die Überlappung der Schwankungsbereiche geringer wird, je länger der Text ist, und die Schwankung selbst, grob gesagt, mit der Quadratwurzel aus der Textlänge zurückgeht, wie Abb. 108 für das /e/ zeigt.

Um die Situation bei längeren Texten zu studieren, vergleichen wir die auf einer Auszählung von 4 000 000 Zeichen beruhende Häufigkeitsreihenfolge von Meyer-Matyas mit einem ziemlich langen englischen Text[2] von 29 272 Zeichen, dessen Auszählung die in Abb. 109 wiedergegebene Häufigkeitsverteilung hat. Abb. 110 zeigt die sich ergebende Gegenüberstellung. Es gibt weit weniger Überkreuzungen, aber es kommen immer noch solche vor.

3879	2697	2240	2151	2133	2082	1910	1907	1415	1095	1035	995	780
e	t	a	n	o	i	r	s	h	d	l	c	m
765	719	687	620	551	469	404	277	230	101	55	45	30
u	f	p	y	g	w	b	v	k	x	z	q	j

Abb. 109. Häufigkeitsverteilung in einem langen englischen Text von 29 272 Zeichen

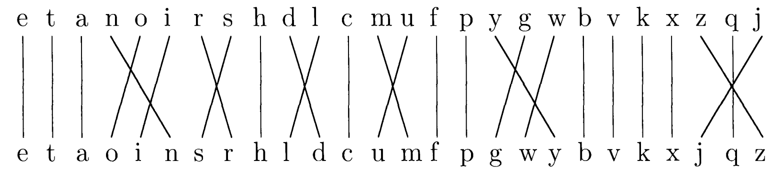


Abb. 110. Gegenüberstellung der Häufigkeitsreihenfolgen für einen langen englischen Text von 29 272 Zeichen (oben) und für die Auszählung von Meyer-Matyas (unten)

[2] Abschnitt 11.2 der englischen Version dieses Buches.

Wenn der lange englische Klartext einer einfachen Substitution unterworfen wird, der Geheimtext dann ausgezählt wird und nach der Häufigkeitsreihenfolge die Dechiffrierung erfolgt, so ergibt sich ein verstümmelter Klartext, der wie folgt beginnt:

```
i v e s t h e c e o t m s n e r c s g p t i d i w g h a r c i d d e c t
e l a t s e a r m s g i f e x p e s n e o c e r e v e o t h e i p e o d
n t e s a t m s e r h i y r t h n r t h e r e e x p e s n e o c e r o i
s u a d d g r c a t t e s e l c a o b e c i o c e o t s a t e l n o t i
a f e y u a x n u r f i s c s g p t i w s a p h n c y i s k n o p a s t
```

Er kann nicht fließend gelesen werden: Wie zu erwarten, muß i durch /o/, s durch /r/, o durch /n/, m durch /u/, n durch /i/, r durch /s/, usw. ersetzt werden – was nicht auf den ersten Blick gelingt. Der wahre Text lautet:

```
o v e r t h e c e n t u r i e s c r y p t o l o g y h a s c o l l e c t
e d a t r e a s u r y o f e x p e r i e n c e s e v e n t h e o p e n l
i t e r a t u r e s h o w s t h i s t h e s e e x p e r i e n c e s n o
r m a l l y s c a t t e r e d c a n b e c o n c e n t r a t e d i n t o
a f e w m a x i m s f o r c r y p t o g r a p h i c w o r k i n p a r t
```

15.5.2 Es ist also zweckmäßig, statt mit der Häufigkeitsreihenfolge der Zeichen mit einer Reihenfolge von Cliquen ‚gleichhäufiger' Zeichen zu arbeiten, die auf grund der Beobachtung ihrer Häufigkeit nur schwer trennbar sind.

Für die deutsche Sprache gibt es eine Zerlegung des Buchstabenvorrats in Cliquen, die im wesentlichen schon von *André Lange* and *E.-A. Soudart* 1935 angegeben wurde:

{e} {nirsatdhu} {lgocmbfwkz} {pvjyxq} ,

oder etwas feiner zerlegt,

{e} {n} {irsat} {dhu} {lgocm} {bfwkz} {pv} {jyxq} ,

was für lange und nicht ausgefallene Texte noch aufgespalten werden kann in

{e} {n} {ir} {sat} {dhu} {lgo} {cm} {bfwkz} {pv} {jyxq} .

Für die englische Sprache bestätigt sich die schon von *L. D. Smith* 1943 angegebene Partition in Cliquen:

{etaoin} {srh} {ld} {cumfpgwyb} {vk} {xjqz} ,

oder etwas feiner zerlegt,

{e} {t} {aoin} {srh} {ld} {cumf} {pgwyb} {vk} {xjqz} ,

was für lange und nicht ausgefallene Texte noch aufgespalten werden kann in

{e} {t} {ao} {in} {srh} {ld} {cu} {mf} {p} {gwy} {b} {v} {k} {xjqz} .

Es ist somit ein interaktives Vorgehen angezeigt, das die Cliquen eine nach der anderen behandelt. Insbesondere wenn die Zerlegung fein genug ist, um Cliquen von nur zwei oder drei Elementen zu erlauben, ist der exhaustive

Aufwand machbar. Für das Beispiel des englischen Textes (Abb. 110) sind die Cliquen in Abb. 111 gegenübergestellt; um die 15 häufigsten Buchstaben auszurichten, wären theoretisch $4! \times 3! \times 2! \times 4! = 6\,912$ Versuche auszuführen.

{e} {t} {a} {noi} {rs} {h} {dl} {c} {mufp} {ygw} {b} {v} {k} {xzqj}

{e} {t} {aoin} {srh} {ld} {cumf} {pgwyb} {vk} {xjqz}

Abb. 111. Gegenüberstellung der Cliquen

In diesem Fall war die Entzifferung immer noch recht gut, weil sich die Cliquen nicht zu sehr überlappten und eine klare Lücke zwischen zwischen /a/ und /n/, zwischen /s/ und /h/ und zwischen /c/ and /m/ bestand. In solchen Fällen sind praktisch nur wenige Versuche notwendig.

15.5.3 Für den kurzen Geheimtext ‚Böll' von 15.3.1 mit den Häufigkeiten in Abb. 103 zeigt Abb. 112 die Gegenüberstellung der Cliquen. Eine so feine Zerlegung in Cliquen wie eben gelingt nicht: 54 H und 41 Q legen nahe H≙e and Q≙n, aber angesichts der nächsten Häufigkeiten 36 D, 24 W, 23 L, 22 V, and 21 K, kann eine Separation der Cliquen {ir} und {sat} nicht erfolgen. Aber D ist wohlsepariert und es sieht vielversprechend aus, D≙i zu setzen. Das würde {rsat} mit {WLVK} konfrontieren, was 4!=24 Versuche bedeutet. Unglücklicherweise gibt keiner von diesen einen vernünftigen Text. In der Tat sind die nächsten beiden Häufigkeiten 19 U und 18 X so nahe, daß eine Überkreuzung in die Clique {dhu} möglich wäre. All dies würde bedeuten, daß $8! = 40\,320$ Versuche erforderlich wären, was außerhalb der Machbarkeit der Exhaustion liegt. Für kurze Texte, selbst wenn sie einfach monoalphabetisch chiffriert sind, gelingt eine rein mechanische Entziffeрung nicht. Zumindest müssen andere stochastische Eigentümlichkeiten der Sprache, wie Bigrammhäufigkeiten, in Betracht gezogen werden (siehe 15.7).

{H} {Q} {D} {L U V W K X} {G O J F P E I N} {R Z C S} {Y M B A T}

{e} {n} {i r} {a s t} {h u d} {l g o} {c m} {b f w k z} {p v} {j y x q}

Abb. 112. Gegenüberstellung der Cliquen für den Geheimtext ‚Böll' von 15.3.1

15.5.4 Für die englische Sprache gibt Tabelle 8 empirische relative Häufigkeiten $\mu_i = m_i/M$ als Resultat einer Auszählung durch *Meyer & Matyas*, basierend auf $M = 4\,000\,000$ Zeichen in einem Korpus von Alltagsenglisch. *Solomon Kullback* hat 1976 darauf hingewiesen, daß das Genre der Kommunikation zu starken Schwankungen führt, und unterscheidet *'literary English'* mit einer Häufigkeit für /e/ von 12.77% von *'telegraphic English'* mit einer Häufigkeit für /e/ von 13.19%. Für die deutsche Sprache liefert die schon erwähnte Textbasis *SZ3-92* mit insgesamt $M = 681\,972$ Zeichen Resultate, die ebenfalls in Tabelle 8 verzeichnet sind. Die Häufigkeit von /e/ ist verzerrt durch die kryptographische Gewohnheit, /ä/, /ö/, /ü/ in /ae/, /oe/, /ue/ zu zerlegen. Die numerischen Werte in Tabelle 8 können als hypothetische Wahrscheinlichkeitsverteilung einer stochastischen Quelle dienen.

George K. Zipf und *Benoît Mandelbrot* haben empirische Formeln für die relative Häufigkeit des k-ten Buchstaben gegeben, die viele Sprachen erstaunlich gut treffen, nämlich

$$p(k) \propto 1/k \quad \text{und} \quad p(k) \propto 1/(k+c)^m \quad \text{für geeignete positive } c, m \; .$$

Die tatsächlichen, empirischen Häufigkeiten sind in Abb. 113a, 113b graphisch aufgetragen. Eine überzeugende theoretische Erklärung liegt nicht vor.

Zeichen	englisch	deutsch	Zeichen	englisch	deutsch
a	8.04%	6.47%	n	7.09%	9.84%
b	1.54%	1.93%	o	7.60%	2.98%
c	3.06%	2.68%	p	2.00%	0.96%
d	3.99%	4.83%	q	0.11%	0.02%
e	12.51%	17.48%	r	6.12%	7.54%
f	2.30%	1.65%	s	6.54%	6.83%
g	1.96%	3.06%	t	9.25%	6.13%
h	5.49%	4.23%	u	2.71%	4.17%
i	7.26%	7.73%	v	0.99%	0.94%
j	0.16%	0.27%	w	1.92%	1.48%
k	0.67%	1.46%	x	0.19%	0.04%
l	4.14%	3.49%	y	1.73%	0.08%
m	2.53%	2.58%	z	0.09%	1.14%

Tabelle 8. Hypothetische Zeichenwahrscheinlichkeiten im Englischen und im Deutschen

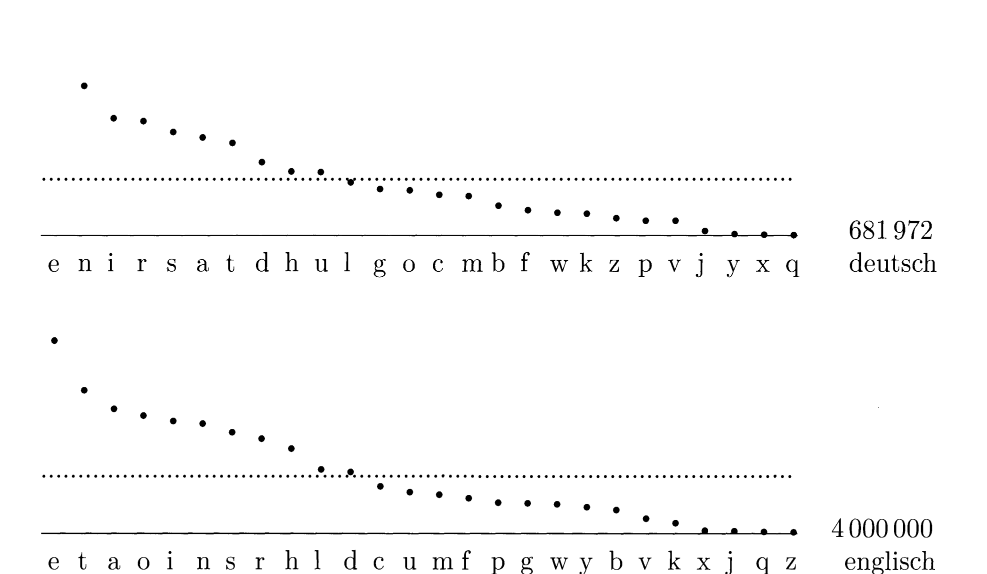


Abb. 113. Häufigkeiten der Einzelzeichen im Deutschen (Textbasis *SZ3-92*) und im Englischen (Auszählung Meyer-Matyas)

15.6 Abstandsminimierung

15.6.1 Wir schließen an 15.2 an. Es sei M die Länge eines Textes T aus einer stochastischen Quelle Q mit den Wahrscheinlichkeiten p_i für das Auftreten des i-ten Zeichens χ_i $(i = 1 \ldots N)$; m_i sei die beobachtete Häufigkeit von χ_i im Text T, wobei $\sum_{i=1}^{N} m_i = M$. Die Häufigkeits-Abweichung des tatsächlichen Textes T von einem zu erwartenden Text T^Q gleicher Länge kann gemessen werden durch das **Abstandsquadrat**

$$d(T, T^Q) = \sum_{i=1}^{N}(m_i - M \cdot p_i)^2 \quad .$$

σ sei die Substitution, die die Geheimtextzeichen in die Klartextzeichen überführt. Der Wert von

$$d_\sigma = d(T, T^{\sigma(Q)}) = \sum_{i=1}^{N}(m_i - M \cdot p_{\sigma(i)})^2$$

ist ein Maß für die Übereinstimmung zwischen dem Geheimtext T mit den Häufigkeiten m_i und dem zu erwartenden Geheimtext $T^{\sigma(Q)}$ der Quelle $\sigma(Q)$;

$$\min_\sigma d_\sigma = \min_\sigma \sum_{i=1}^{N}(m_i - M \cdot p_{\sigma(i)})^2$$

charakterisiert die Substitutionen, die bestmögliche Übereinstimmung bringen und damit Kandidaten für die Entzifferung sind. Wegen der auftretenden Schwankungen sind aber auch Substitutionen σ, für die d_σ in die Nähe des Minimums kommt, in Betracht zu ziehen, wobei sie mit wachsender Entfernung vom Minimum weniger und weniger in Frage kommen.

15.6.2 Offensichtlich gilt $\quad \sum_{i=1}^{N} p_{\sigma(i)}^2 = \sum_{i=1}^{N} p_i^2 \quad$ und damit

$$\min_\sigma \sum_{i=1}^{N}(m_i - M \cdot p_{\sigma(i)})^2 = \sum_{i=1}^{N} m_i^2 + M^2 \sum_{i=1}^{N} p_i^2 - 2M \max_\sigma \sum_{i=1}^{N} m_i \cdot p_{\sigma(i)} \; .$$

Zur Entzifferung genügt es also, folgendes Maximum zu suchen:

$$\max_\sigma \sum_{i=1}^{N} m_i \cdot p_{\sigma(i)} \; .$$

Satz: Es sei für alle $i \quad m_i \geq m_{i+1}$.
$\sum_{i=1}^{N} m_i \cdot p_{\sigma(i)}$ wird genau dann maximal, wenn für alle $i \;\; p_{\sigma(i)} \geq p_{\sigma(i+1)}$.

> Beweis: Da jede Permutation als Kette zweigliedriger Vertauschungen dargestellt werden kann, genügt es, den Beitrag zweier Zeichen χ_j, χ_k zur Summe zu betrachten. Dann ist
>
> $m_j \cdot p_{\sigma(j)} + m_k \cdot p_{\sigma(k)} \geq m_j \cdot p_{\sigma(k)} + m_k \cdot p_{\sigma(j)}$ genau dann, wenn
> $(m_j - m_k) \cdot (p_{\sigma(j)} - p_{\sigma(k)}) \geq 0$, d.h. wenn $p_{\sigma(j)} \geq p_{\sigma(k)}$. ⋈

Es ergibt sich also das erwartete Resultat, daß theoretisch die Entzifferung gelingen sollte mit einer Zuordnung nach der Häufigkeitsreihenfolge. Wegen der auftretenden Schwankungen ist das praktisch nur ungefähr richtig; es empfiehlt sich daher, von diesen Zuordnungen ausgehend paarweise Zeichen χ_j, χ_k zu vertauschen, beginnend mit möglichst kleinen Werten von

$$(m_j - m_k) \cdot (p_{\sigma(j)} - p_{\sigma(k)}) \; .$$

Beispiel:

Mit den Wahrscheinlichkeiten p_i von Tabelle 8 und der daraus resultierenden Häufigkeitsreihenfolge ergibt sich für den Geheimtext ‚Böll' von 15.3.1 mit den in Abb. 103 angegebenen Häufigkeiten m_i und einer Zuordnung nach deren Häufigkeitsreihenfolge für $\sum_{i=1}^{N} m_i \cdot p_{\sigma(i)}$ ein Wert von

$$2634.56\% = M \cdot 7.5489\% \;;$$

vertauscht man die Zuordnung $\mathrm{D} \hat{=} \mathrm{i}$, $\mathrm{W} \hat{=} \mathrm{r}$ zu der nach der Reihenfolge von *Kaeding* auftretenden $\mathrm{D} \hat{=} \mathrm{r}$, $\mathrm{W} \hat{=} \mathrm{i}$; so wird der Wert geringfügig geringer um $(36-24) \cdot (7.73\% - 7.54\%) = 2.28\% = M \cdot 0.0065\%$ und wird

$$2632.28\% = M \cdot 7.5424\% \;.$$

Für die tatsächliche Entzifferung errechnet sich ein Wert von nur

$$2585.80\% = M \cdot 7.4092\%.$$

Der Wert von $\sum_{i=1}^{N} m_i^2$ in diesem Beispiel ist $9347 = M^2 \cdot 7.67\%$, der Wert von $\sum_{i=1}^{N} p_i^2$ nach Tabelle 8 beträgt 7.62%.

	.a	.b	.c	.d	.e	.f	.g	.h	.i	.j	.k	.l	.m	.n	.o	.p	.q	.r	.s	.t	.u	.v	.w	.x	.y	.z
a.	8	31	27	11	64	15	30	20	5	1	7	59	28	102		4		51	53	46	75	2	3		1	2
b.	16	1		1	101		3	1	12		1	9		1	8			9	6	4	14		1		1	1
c.	2			2	1			242	1		14	1			2				1							
d.	54	3	1	13	227	3	4	2	93	1	3	5	4	6	9	3		10	11	6	16	3	4			3
e.	26	45	25	51	23	26	50	57	193	3	19	63	55	400	6	13	1	409	140	55	36	14	23	2	1	11
f.	19	2		9	25	12	3	1	7		1	5	1	2	9	1		18	4	20	24	1	1			1
g.	20	3		12	147	2	3	3	19	1	3	9	3	5	6	1		14	18	18	11	4	3			3
h.	70	4	1	14	102	2	4	3	23	1	3	25	11	19	18	1		37	11	47	11	4	9			3
i.	7	7	76	20	163	5	38	12	1	1	12	25	27	168	20	2		17	79	78	3	5	1			5
j.	9				9										2						5					
k.	26	1		2	26	1	1	1	7		1	10	1	1	24	1		13	5	14	9	1	1			1
l.	45	7	2	14	65	5	6	2	61	1	7	42	3	4	14	2		2	22	27	13	3	2			3
m.	40	6	1	8	50	4	4	3	44	2	3	4	23	3	15	7		2	10	8	14	4	3			2
n.	68	23	5	187	122	19	94	17	65	5	25	10	23	43	18	10		10	74	59	33	18	29			25
o.	3	8	15	7	25	6	5	9	1	1	3	31	17	64	1	6		50	19	9	3	3	7		1	6
p.	16			3	10	6		2	4			4			11	5		23	1	3	4					
q.																					2					
r.	80	25	9	67	112	18	27	19	52	4	23	18	20	31	30	9		15	54	49	48	12	17			14
s.	36	10	89	20	99	7	13	9	65	2	11	9	12	7	28	22		8	76	116	15	9	10		2	7
t.	57	8	1	35	185	5	10	14	59	2	4	11	9	9	15	3		31	50	23	26	8	21		1	26
u.	3	8	16	5	78	27	8	4	2		3	7	21	119		5		33	48	23	1	3	2			1
v.	3				37				9						43											
w.	34				48				36	1				1	17				1		9					
x.									1						1					1						
y.					1							1	1						1							
z.	4	1		1	28		1		11		1	2	1		2				1	7	43	1	9			1

Tabelle 9. Bigramm-Häufigkeiten (in %%) im Deutschen (Textbasis *SZ3-92*)

15.7 Häufigkeit von Multigrammen

Noch mehr als die Einzelzeichenhäufigkeit prägt die Häufigkeit von Multigrammen eine Sprache. Die Multigramm-Häufigkeiten sind auch wesentlich weniger ausgeglichen. In kurzen Texten treten jedoch schon Bigramme so selten auf, daß die Schwankungseinflüsse erheblich sind.

Invarianzsatz $3^{(n)}$: Für alle monoalphabetischen, funktionalen einfachen Substitutionen , insbesondere auch für alle linearen monoalphabetischen einfachen Substitutionen gilt:
Partitionen der n-gramme innerhalb des Textes bleiben erhalten.

15.7.1 Damit kann auch die Häufigkeit von n-grammen in einem Geheimtext zur Entzifferung herangezogen werden. Allerdings gibt es für $N=26$ bereits 676 Bigramme und 17 576 Trigramme; nur bei recht langen Geheimtexten wird man also einigermaßen genügend viele Bigramme und Trigramme finden. Eine Kryptanalyse monographischer Chiffrierungen aufgrund etwa von Bigrammen allein an Stelle von Einzelzeichen bringt keine großen Vorteile.

	.a	.b	.c	.d	.e	.f	.g	.h	.i	.j	.k	.l	.m	.n	.o	.p	.q	.r	.s	.t	.u	.v	.w	.x	.y	.z
a.	1	32	39	15		10	18		16		10	77	18	172	2	31	1	101	67	124	12	24	7		27	1
b.	8				58				6	2		21	1		11			6	5		25				19	
c.	44		12		55	1		46	15		8	16			59	1		7	1	38	16		1			
d.	45	18	4	10	39	12	2	3	57	1		7	9	5	37	7	1	10	32	39	8	4	9		6	
e.	65	11	64	107	39	23	20	15	40	1	2	46	43	120	46	32	14	154	145	80	7	16	41	17	17	
f.	21	2	9	1	25	14	1	6	21	1		10	3	2	38	3		4	8	42	11	1	4		1	
g.	11	2	1	1	32	3	1	16	10			4	1	3	23	1		21	7	13	8		2		1	
h.	84	1	2	1	251	2		5	72			3	1	2	46	1		8	3	22	2		7		1	
i.	18	7	55	16	37	27	10				8	39	32	169	63	3		21	106	88		14	1	1		4
j.					2										4						4					
k					28				8					3	3				2	1			3		3	
l.	34	7	8	28	72	5	1		57	1	3	55	4	1	28	2	2	2	12	19	8	2	5		47	
m.	56	9	1	2	48			1	26				5	3	28	16			6	6	13		2		3	
n.	54	7	31	118	64	8	75	9	37	3	3	10	7	9	65	7		5	51	110	12	4	15	1	14	
o.	9	18	18	16	3	94	3	3	13		5	17	44	145	23	29		113	37	53	96	13	36		4	2
p.	21	1			40			7	8			29			28	26	42	3	14	7		1		2		
q.																					20					
r.	57	4	14	16	148	6	6	3	77	1	11	12	15	12	54	8		18	39	63	6	5	10		17	
s.	75	13	21	6	84	13	6	30	42		2	6	14	19	71	24	2	6	41	121	30	2	27		4	
t.	56	14	6	9	94	5	1	315	128			12	14	8	111	8		30	32	53	22	4	16		21	
u.	18	5	17	11	11	1	12	2	5			28	9	33	2	17		49	42	45				1	1	1
v.	15				53				19						6											
w.	32		3	4	30	1		48	37			4	1	10	17	2		1	3	6	1	1	2			
x.	3		5		1				4						1	4				1	1					
y.	11	11	10	4	12	3	5	5	18			6	4	3	28	7		5	17	21	1	3	14			
z.					5				2			1														1

Tabelle 10. Bigramm-Häufigkeiten (in %%) im Englischen (nach *O. Phelps Meaker*)

Die Häufigkeit von Bigrammen (einen Anhaltspunkt dafür geben Tabelle 9 und Tabelle 10) und Trigrammen zeigt noch mehr Unausgeglichenheit[3] als die von Einzelzeichen. Die 18 häufigsten Bigramme im Deutschen (sie machen 92.93% aller Bigramme aus) und die 19 häufigsten Bigramme im Englischen zeigen Tabelle 11 und Tabelle 12; die 112 häufigsten Trigramme im Deutschen (sie machen aber nur noch 52.11% aller Trigramme aus) und die 98 häufigsten Trigramme im Englischen finden sich in Tabelle 13 und Tabelle 14. Die Auszählungen streuen überdies sehr, wie man unschwer aus Tabelle 11 und Tabelle 12 ersieht.[4] Tabelle 9 und Tabelle 10 zeigen auch auf einen Blick, daß die Bigramm-Häufigkeitsmatrix nicht symmetrisch ist. Häufig vorkommende Bigramme mit seltenen Reversen (‚Drehern') sind

/th/, /he/, /ea/, /nd/, /nt/, /ha/, /ou/, /ng/, /hi/, /eo/, /ft/, /sc/, /rs/ ,

sie sind zum Auflösen von Cliquen nützlich. Dagegen kommen folgende Bigramme ungefähr gleich häufig vor:

/er/ - /re/, /es/ - /se/, /an/ - /na/, /ti/ - /it/, /on/ - /no/, /in/ - /ni/, /en/ - /ne/, /at/ - /ta/, /te/ - /et/, /or/ - /ro/, /to/ - /ot/, /ar/ - /ra/, /st/ - /ts/, /is/- /si/, /ed/ - /de/, /of/ - /fo/ .

	Tabelle 9	Bauer-Goos	Valerio	Eyraud
er	409	340	337	375
en	400	447	480	443
ch	242	280	266	280
de	227	214	231	233
ei	193	226	187	242
nd	187	258	258	208
te	185	178	222	178
in	168	204		197
ie	163	176	222	188
ge	147	168	160	196
es	140	181		168
ne	122	117		143
un	119	173	169	139
st	116	124		118
re	112	107	213	124
he	102	117		124
an	102	92		82
be	101	96		104

Tabelle 11. Die achtzehn häufigsten Bigramme im Deutschen (Häufigkeiten in %%)

[3] Beim Vergleich von Werten in der Literatur ist darauf zu achten, ob der Wortzwischenraum unberücksichtigt bleibt; gelegentlich (so bei *Fletcher Pratt* 1939) werden nur Bigramme und Trigramme innerhalb von Wörtern gezählt.

[4] Häufigkeitstabellen für eine Reihe von indogermanischen Sprachen finden sich insbesondere bei *H. F. Gaines* und bei *Ch. Eyraud.*

	Tabelle 10	Kullback	Sinkov	Eyraud
th	315	156	270	330
he	251	40	257	270
an	172	128	152	167
in	169	150	194	202
er	154	174	179	191
re	148	196	160	169
on	145	154	154	134
es	145	108	115	149
ti	128	90	108	126
at	124	94	127	127
st	121	126	103	116
en	120	222	129	146
or	113	128	108	91
nd	118	104	95	122
to	111	100	95	79
nt	110	164	93	124
ed	107	120	111	125
is	106	70	93	79
ar	101	88	96	83

Tabelle 12. Die neunzehn häufigsten Bigramme im Englischen (Häufigkeiten in %%)

15.7.2 Nicht uninteressant sind auch die Häufigkeiten des Vorkommens von Wörtern. Die zehn häufigsten Wörter sind

im Deutschen: die der und den am in zu ist daß es ,
im Englischen: the of and to a in that it is I ,
im Französischen: de il le et que je la ne on les ,
im Italienischen: la di che il non si le una lo in ,
im Spanischen: de la el que en no con un se sa .

Einbuchstabige Wörter sind im Englischen nur a und I , zweibuchstabig sind an at as he be in is it on or to of do go no so my .

Die häufigsten Wörter in den indogermanischen Sprachen sind weit überwiegend **Formwörter**[5] (*mots vides*, *non-content words*, „inhaltsleere Wörter“), nämlich Artikel, Präpositionen, Konjunktionen und andere Hilfspartikel, im Gegensatz zu **Begriffswörtern** wie Substantiven, Adjektiven und Verben. Unter den 70 häufigsten Wörtern der englischen Sprache sind keine Begriffswörter, unter den 100 häufigsten sind nur 10 Begriffswörter.

15.7.3 Die Häufigkeit eines Buchstabens hängt oft sehr von seiner Lage im Wort ab. Beispielsweise steht /e/ im Deutschen

[5] Im Englischen sind es gerade die Formwörter, die in Überschriften nicht groß geschrieben werden.

ein	122	das	47	erd	33	ese	27	eni	23	ner	20	hei	18
ich	111	hen	47	enu	33	auf	26	ige	23	nds	20	lei	18
nde	89	ind	46	nen	32	ben	26	aen	22	nst	20	nei	18
die	87	enw	45	rau	32	ber	26	era	22	run	20	nau	18
und	87	ens	44	ist	31	eit	26	ern	22	sic	20	sge	18
der	86	ies	44	nic	31	ent	26	rde	22	enn	19	tte	18
che	75	ste	44	sen	31	est	26	ren	22	ins	19	wei	18
end	75	ten	44	ene	30	sei	26	tun	22	mer	19	abe	17
gen	71	ere	43	nda	30	and	25	ing	21	rei	19	chd	17
sch	66	lic	42	ter	30	ess	25	sta	21	eig	18	des	17
cht	61	ach	41	ass	29	ann	24	sie	21	eng	18	nte	17
den	57	ndi	41	ena	29	esi	24	uer	21	erg	18	rge	17
ine	53	sse	39	ver	29	ges	24	ege	20	ert	18	tes	17
nge	52	aus	36	wir	29	nsc	24	eck	20	erz	18	uns	17
nun	48	ers	36	wie	28	nwi	24	eru	20	fra	18	vor	17
ung	48	ebe	35	ede	27	tei	24	mme	20	hre	18	dem	17

Tabelle 13. Die 112 häufigsten Trigramme im Deutschen (Häufigkeiten in %%)

the	353	hat	55	man	40	ant	32	rom	28	str	25	nte	23
ing	111	ers	54	red	40	hou	31	ven	28	tic	25	rat	23
and	102	his	52	thi	40	men	30	ard	28	ame	24	tur	23
ion	75	res	50	ive	38	was	30	ear	28	com	24	ica	23
tio	75	ill	47	rea	38	oun	30	din	27	our	24	ich	23
ent	73	are	47	wit	37	pro	30	sti	27	wer	24	nde	23
ere	69	con	46	ons	37	sta	30	not	27	ome	24	pre	23
her	68	nce	45	ess	36	ine	29	ort	27	een	24	enc	22
ate	66	all	44	ave	34	whi	28	tho	26	lar	24	has	22
ver	64	eve	44	per	34	ove	28	day	26	les	24	whe	22
ter	63	ith	44	ect	33	tin	28	ore	26	san	24	wil	22
tha	62	ted	44	one	33	ast	28	but	26	ste	24	era	22
ati	59	ain	43	und	33	der	28	out	25	any	23	lin	22
for	59	est	42	int	32	ous	28	ure	25	art	23	tra	22

Tabelle 14. Die 98 häufigsten Trigramme im Englischen (Häufigkeiten in %%)

an erster Stelle	7.7%	an drittletzter Stelle	8.8%
an zweiter Stelle	21.7%	an vorletzter Stelle	7.7%
an dritter Stelle	16.5%	an letzter Stelle	15.0%

.

15.7.4 Auch wenn man (oder gerade weil man) professionell den Wortzwischenraum unterdrückt, ist die mittlere Wortlänge eine nicht unwichtige Kenngröße einer Sprache, sowie die Vokalhäufigkeit und die Häufigkeit der fünf häufigsten Konsonanten {lnrst}. Angaben dazu finden sich in Tabelle 15.

Im Deutschen sind die Wortlängenhäufigkeiten folgendermaßen verteilt:

1	0.05%	6	11.66%	11	3.24%	16	0.32%
2	8.20%	7	6.04%	12	2.06%	17	0.38%
3	28.71%	8	4.43%	13	1.40%	18	0.16%
4	13.49%	9	3.67%	14	0.59%	19	0.10%
5	11.55%	10	2.64%	15	0.65%		

15.7.5 Vokale und Konsonanten wechseln sich oft gegenseitig ab. Vokale bilden das sangliche Lautgerüst einer Sprache. Im Französischen können sie sehr gehäuft auftreten: *ouïe, aïeul.* Konsonanten, die im Arabischen das Schreibgerüst einer Sprache bilden, treten in slawischen Sprachen ebenfalls oft gehäuft auf: *czyszczenie* (polnisch), *cvŕčak* (serbokroatisch), *nebezpečenství* (tschechisch). Im Walisischen kommen noch seltsamere Wortungetüme vor: *Llanfairpwllgwyngyllgogerychwyrndrobwllllantysiliogogogoch* ist der Name einer Bahnstation. Auch *rhy ddrwg* (‚zu dumm') ist bemerkenswert: *y* und *w* bezeichnen Vokale. Im Englischen sind Wörter mit 4-Konsonanten-Folgen wie *sixths* sehr selten; im Deutschen sind *Schlacht, schlecht, schlicht, Schlucht* achtbuchstabige Wörter mit nur einem Vokal, durch Zusammensetzung erhält man Wörter mit 7-Konsonanten-Folgen wie *Erstschlag*. Auch Vokalabstände haben typische Häufigkeiten: Im Deutschen (ohne Zwischenräume)

1	20.77%	5	2.63%
2	25,06%	6	1.03%
3	35.95%	7	0.15%
4	14.75%	8	0.03%

.

15.7.6 Für *informal ciphers*, die Wortzwischenräume (und eventuell auch Interpunktionen) beibehalten, enthalten Bigrammtabellen natürlich auch Häufigkeiten für an- und auslautende Buchstaben, Trigrammtabellen Häufigkeiten für an- und auslautende Bigramme und für einbuchstabige Wörter. Werden Zwischenräume (und Interpunktionen) nicht unterdrückt, so müssen sie zumindest in die Chiffrierung einbezogen werden; damit wird der Zwischenraum zum häufigsten Zeichen, geringfügig häufiger als das /e/ .

Werden aber Zwischenräume (und Interpunktionen) durch sich selbst chiffriert, wie das für die *aristocrats* üblich ist, läuft das darauf hinaus, daß *ein* Zeichen von vornherein entziffert ist. Das erleichtert natürlich jeden Einstieg ganz bedeutend. Erfahrene Kryptologen lesen solche *informal ciphers* manchmal auf den ersten Blick (*"Not infrequently, the cryptogram which retains its word-divisions can be read at sight ... and this regardless of how short it may be"* — *Helen Fouché Gaines* 1939).

In der professionellen Kryptologie verwendet man jedenfalls, wie wir es getan haben, aus guten Gründen *formal ciphers*. Wenn aus technischen Gründen, wie im Fernschreibbetrieb und bei Verwendung eines ASCII-Codes, Sonderzeichen verfügbar sind, so heißt das noch lange nicht, daß sie bedenkenlos benutzt werden müssen — ein gut ausgebildeter und verantwortungsbewußter Kryptosekretär wird das wissen.

	mittlere Wortlänge	Vokal-häufigkeit	{lnrst}-Häufigkeit	seltene Buchstaben						
engl.	4.5	40%	33%	j		q		x		z
dtsch.	5.9	39%	34%	j		q		x	y	
franz.	4.4	45%	34%		k		w			
ital.	4.5	48%	30%	j	k		w	x	y	
span.	4.4	47%	31%		k		w			
russ.	6.3	45%								

Tabelle 15. Kenngrößen verschiedener Sprachen

15.8 Die kombinierte Methode der Häufigkeitserkennung

Zur Mechanisierung der Entzifferung monoalphabetischer einfacher Substitutionen, insbesondere bei kürzeren Texten in einer bekannten Sprache, ist es angezeigt, die Häufigkeiten von Einzelzeichen, von Bigrammen und eventuell von Trigrammen kombiniert heranzuziehen, und zwar so, daß man Bigrammhäufigkeiten betrachtet, wenn eine Clique von Zeichen durch Einzelhäufigkeiten nicht getrennt werden kann; Trigrammhäufigkeiten betrachtet, wenn eine Clique von Bigrammen durch Bigrammhäufigkeiten nicht getrennt werden kann. Über Trigramme wird man nicht gerne hinausgehen. Sofern dabei keine Mustererkennungstechniken (‚wahrscheinliche Wörter‘) herangezogen werden, spricht man von *ciphertext-only attack* und *pure cryptanalysis*, die nur eine Annahme über die vorliegende Sprache braucht.

15.8.1 Für folgenden Geheimtext von 280 Zeichen (*Kahn* 1967)

```
GJXXN GGOTZ NUCOT WMOHY JTKTA MTXOB
YNFGO GINUG JFNZV QHYNG NEAJF HYOTW
GOTHY NAFZN FTUIN ZANFG NLNFU TXNXU
FNEJC INHYA ZGAEU TUCQG OGOTH JOHOA
TCJXK HYNUV OCOHQ UHCNU GHHAF NUZHY
NCUTW JUWNA EHYNA FOWOT UCHNP HOGLN
FQZNG OFUVC NZJHT AHNGG NTHOU CGJXY
OGHTN ABNTO TWGNT HNTXN AEBUF KNFYO
HHGIU TJUCE AFHYN GACJH OATAE IOCOH
UFQXO BYNFG
```

ergibt die Häufigkeitszählung der Buchstaben

17	4	13	0	7	17	23	26	5	12	3	2	2	36	25	1	5	0	0	23	20	3	6	9	13	8
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Es besteht kein Anklang an ein verschobenes Häufigkeitsgebirge, es darf also nicht mit dem Vorliegen einer CAESAR-Addition gerechnet werden. Die Häufigkeitsreihenfolge ist

36	26	25	23	23	20	17	17	13	13	12	9	8	7	6	5	5	4	3	3	2	2	1	0	0	0
N	H	O	G	T	U	A	F	C	Y	J	X	Z	E	W	I	Q	B	K	V	L	M	P	D	R	S

	e	t	a	o	n	i	r	s	h	l	d	u	c
e	39	80	131	46	120	40	154	145	15	46	107	7	64
t	94	53	56	111	8	128	30	32	315	12	9	22	6
a	–	124	1	2	172	16	101	67	–	77	15	12	39
o	3	53	9	23	145	13	113	37	3	17	16	96	18
n	64	110	54	65	9	37	5	51	9	10	118	12	31
i	37	88	18	63	169	–	21	106	–	39	16	–	55
r	148	63	57	54	12	77	18	39	3	12	16	6	14
s	84	121	75	71	19	42	18	41	30	6	6	30	21
h	251	22	84	46	2	72	8	3	5	3	1	2	2
l	72	19	34	28	1	57	2	12	–	55	28	8	8
d	39	39	45	37	5	57	10	32	3	7	10	8	4
u	11	45	18	2	33	5	49	42	2	28	11	–	17
c	55	38	44	59	–	15	7	1	46	16	–	16	12

Tabelle 16. Bigrammtabelle für die 13 häufigsten Buchstaben im Englischen

	N	H	O	G	T	U	A	F	C	Y	J	X	Z
N	–	1	–	5	4	5	5	7	1	–	–	1	3
H	3	2	4	1	2	1	1	–	1	9	1	–	–
O	–	4	–	4	7	1	2	1	2	–	–	–	–
G	4	2	6	2	–	–	2	–	–	–	3	–	–
T	1	4	1	–	–	3	3	–	1	–	1	3	1
U	–	1	–	2	4	–	–	3	5	–	–	–	1
A	1	1	–	–	2	–	–	4	1	–	1	–	1
F	3	2	1	2	1	2	–	–	–	1	–	–	1
C	2	1	4	1	–	1	–	–	–	–	2	–	–
Y	7	–	3	–	–	–	1	–	–	–	1	–	–
J	–	2	2	–	1	2	–	2	1	–	–	3	–
X	3	–	2	–	–	1	–	–	–	1	–	1	–
Z	3	1	–	1	–	–	1	–	–	–	1	–	–

Tabelle 17. Bigramm-Auszählung, geordnet nach Einzelzeichenhäufigkeit

Den Umständen nach ist zu erwarten, daß es sich um einen englischen Text handelt. Eine Gegenüberstellung mit der Häufigkeitsreihenfolge des Englischen nach *Kahn*

e t a o n i r s h d l u c m p f y w g b v j k q x z .

legt angesichts des deutlichen Abfalls von 17 auf 13 zumindest eine Cliquenbildung {e} {t} {aonirs} nahe. Es sollte also

$\text{N} \mathrel{\hat{=}} \text{e}$, $\text{H} \mathrel{\hat{=}} \text{t}$ und $\{\text{OGTUAF}\} \mathrel{\hat{=}} \{\text{aonirs}\}$ sein.

Zur Auflösung der letzteren Unsicherheit setzt nun die Betrachtung der Bigrammhäufigkeit ein. Tabelle 16 zeigt den relevanten Ausschnitt aus einer Bigrammtabelle für die englische Sprache (10 000 Zeichen), Tabelle 17 die Bigramm-Auszählung des Textes, geordnet nach Einzelzeichenhäufigkeit.

Tabelle 16 zeigt, daß /a/, /i/ und /o/ untereinander Kontakt (engl. *affinity*) meiden, mit Ausnahme des Bigramms /io/ . /oi/ kommt jedoch nur selten vor. In der Auszählung, Tabelle 17, meiden O, U und A ebenfalls Kontakt, OA kommt zweimal vor gegenüber keinmal AO. Es sollte also

O ≙ i , A ≙ o und somit auch U ≙ a

gelten. Daß dann zu OU gerade /ia/ gehört, das häufig vorkommt, paßt. Überdies kommt NU, das für /ea/ stünde, häufig vor, während UN, das gar nicht vorkommt, für das seltene /ae/ stünde. Damit wäre die umfangreiche Clique {aonirs} aufgespalten und es verbleibt nur noch die Clique {GTF}≙{nrs}, die sogar exhaustiv behandelt werden könnte.

Die hier getroffene Argumentation betrifft Zeichen, die Kontakt meiden. Daß dies gerade Vokale sind, ist eine Eigentümlichkeit des Englischen; die in der angelsächsischen Literatur zu findende Bezeichnung 'Vowel-Solution Method' (*Helen Fouché Gaines* 1939) ist also akzidentell. In anderen Sprachen haben Vokale durchaus keine Tendenz, Kontakt zu vermeiden.

Übrigens zeigt auch der Konsonant /n/ Kontakteigentümlichkeiten: /n/ geht sehr häufig ein Vokal voraus. Dies zeichnet T vor G, F und der Clique {C, Y} aus. Also steht zu vermuten, daß

T ≙ n

gilt. Für /r/ und /s/ ist weniger zu gewinnen. Am auffallendsten ist /h/: /th/ ist überaus häufig, /he/ und /ha/ sind häufig. Die noch verbleibenden G, F und C zeigen keine entsprechenden Kontakte; dies legt nahe, daß

Y ≙ h

gilt. Tatsächlich erfüllt Y das Verlangte: HY (für /th/) kommt sehr häufig, YN (für /he/) und YO (für /ha/) kommen häufig vor.

Damit haben wir sieben der zehn häufigsten Geheimtextzeichen bestimmt:

N H U A T O * * Y * * * * * * * * * * * * * * * * *
e t a o n i r s h d l u c m p f y w g b v j k q x z .

15.8.2 Die Lösung sollte nach diesem etwas mühseligen Einstieg „im Trab" gehen. Tatsächlich ergibt sich aus dem bereits Erreichten

GJXXe GGinZ eaCin WMith JnKno MnXiB
heFGi GIeaG JFeZV QtheG eEoJF thinW
Ginth eoFZe FnaIe ZoeFG eLeFa nXeXa
FeEJC Ietho ZGoEa naCQG iGint Jitio
nCJXK theaV iCitQ atCea GttoF eaZth
eCanW JaWeo Etheo FiWin aCteP tiGLe
FQZeG iFaVC eZJtn oteGG entia CGJXh
iGtne oBeni nWGen tenXe oEBaF KeFhi
ttGIa nJaCE oFthe GoCJt ionoE IiCit
aFQXi BheFG .

Einzelne Ergänzungen fallen sofort auf: In der ersten Zeile Mith bedeutet with , woraus M ≙ w ; und JnKnown bedeutet unknown , woraus J ≙ u , K ≙ k . thinW in der zweiten Zeile bedeutet thing , woraus W ≙ g ; in der vierten Zeile bedeutet IethoZ /method/ , woraus I ≙ m , Z ≙ d ; das Wort /intuition/ paßt. Des weiteren sollte man nach Stellen suchen, an denen die noch fehlenden Buchstaben aus der Clique {hdlcwum}, nämlich /l/ und /c/ , vorkommen könnten.

Viel weiter kommt man jedoch mit einer vorherigen Bestimmung von G und F . Man kann nach allem ziemlich sicher sein, daß {GF}≙{rs}. Das Vorkommen von FG in der zweiten Zeile und der Umstand, daß das Bigramm /sr/ sehr selten ist, läßt es wert erscheinen,

G ≙ s , F ≙ r

zu versuchen. Das ergibt die Teilentzifferung

```
suXXe ssind eaCin gwith unkno wnXiB
hersi smeas uredV Qthes eEour thing
sinth eorde rname doers eLera nXeXa
reEuC metho dsoEa naCQs isint uitio
nCuXk theaV iCitQ atCea sttor eadth
eCang uageo Etheo rigin aCteP tisLe
rQdes iraVC edutn otess entia CsuXh
istne oBeni ngsen tenXe oEBar kerhi
ttsma nuaCE orthe soCut ionoE miCit
arQXi Bhers .
```

Nun liest man in der ersten Zeile sJXXess ≙ suXXess als /success/ , woraus X ≙ c , und ZeaCinW ≙ deaCing als /dealing/ , woraus C ≙ l .

Insgesamt kennt man jetzt alle bis auf einige der seltenen Buchstaben:

```
N H U A T O F G Y Z C J X I * * * M W * * * K * * *
e t a o n i r s h d l u c m p f y w g b v j k q x z .
```

Der sich ergebende Text liest sich bereits in flüssigem Galopp:

```
succe ssind ealin gwith unkno wnciB
hersi smeas uredV Qthes eEour thing
sinth eorde rname doers eLera nceca
reEul metho dsoEa nalQs isint uitio
nluck theaV ilitQ atlea sttor eadth
elang uageo Etheo rigin alteP tisLe
rQdes iraVl edutn otess entia lsuch
istne oBeni ngsen tence oEBar kerhi
ttsma nualE orthe solut ionoE milit
arQci Bhers .
```

Der Reihe nach ergänzt man jetzt mühelos B $\hat{=}$ p , V $\hat{=}$ b , Q $\hat{=}$ y , E $\hat{=}$ f; hat dann in der dritten Zeile mit rname doers eLera nceca vielleicht eine Schwierigkeit; findet weiter in der sechsten/siebten Zeile altex tisve rydes , also P $\hat{=}$ x , L $\hat{=}$ v , Q $\hat{=}$ y . Damit findet man auch drei Chiffrierfehler:

In der dritten Zeile muß die vierte Gruppe ZBNFG lauten;
in der siebten Zeile muß die dritte Gruppe NVJHT lauten;
in der achten Zeile muß die erste Gruppe OGHYN lauten.

15.8.3 Wenn das nicht genügen sollte, um die Korrektheit der Entzifferung zu erhärten, so kann man auch noch den Schlüssel aufstellen: Bis auf die drei nicht vorkommenden Buchstaben erhält man

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
U	V	X	Z	N	E	W	Y	O	*	K	C	I	T	A	B	*	F	G	H	J	L	M	P	Q	* .

Das Kennwort NEWYORKCIT(Y) springt ins Auge und liefert noch Chiffren für die drei gar nicht vorkommenden Zeichen R $\hat{=}$ j, D $\hat{=}$ q, S $\hat{=}$ z.

Die Botschaft lautet in menschenfreundlicher Form, Chiffrierfehler bereinigt:

> *"Success in dealing with unknown ciphers is measured by these four things in the order named: perseverance, careful methods of analysis, intuition, luck. The ability at least to read the language of the original text is very desirable, but not essential." Such is the opening sentence of Parker Hitt's "Manual for the Solution of Military Ciphers".*

So nämlich beginnt *Parker Hitts*[6] "Manual for the Solution of Military Ciphers". Der letzte Satz drückt aus, daß semantische Unterstützung nicht ausschlaggebend ist; er sollte als Ermutigung verstanden werden, einen beträchtlichen, wenn auch nicht den wesentlichen Teil der unbefugten Entzifferung maschinell durchführen zu lassen.

Man beachte, daß diese Entzifferung ausschließlich mit Einzelzeichen- und Bigramm-Häufigkeitsbetrachtungen, also aufgrund von Satz 3 und Satz $3^{(2)}$, durchgeführt wurde, und auf naheliegende andere Zugänge, wie Mustererkennung, verzichtet wurde. Über gemischte Methoden mehr in 15.10.

15.8.4 Die korrekte Entzifferung zeigt eine Anpassung der beobachteten Bigrammhäufigkeiten und der auf grund der Wahrscheinlichkeiten erwarteten Häufigkeiten. Tabelle 18 bringt die (gerundeten) Erwartungswerte der Bigrammhäufigkeit für die dreizehn häufigsten Buchstaben im Englischen und die im obigen Beispiel tatsächlich auftretenden Bigrammhäufigkeiten – nach geeigneter Permutation. Eine Anpassung der Bigrammhäufigkeiten hat wie in 15.6 die Aufgabe, Permutationen zu bestimmen, die eine möglichst gute

---

[6] Colonel *Parker Hitt* (1877–1971) publizierte 1916 eines der ersten seriösen Bücher über Kryptologie in den Vereinigten Staaten und beschäftigte sich darin als erster mit der systematischen Entzifferung von PLAYFAIR. 1914 konstruierte er die Streifen-Version von *Bazeries* Zylinder (7.5.3). *Hitt* war später ein Vice-President von AT&T und President von dessen kryptologischer Tochter *International Communication Laboratories*.

	e	t	a	o	n	i	r	s	h	l	d	u	c
e	1.1	2.2	3.7	1.3	3.4	1.1	4.3	4.1	0.4	1.3	3.0	0.2	1.8
t	2.6	1.5	1.6	3.1	0.2	3.6	0.8	0.9	8.8	0.3	0.3	0.6	0.2
a	–	3.5	–	0.1	4.8	0.4	2.8	1.9	–	2.2	0.4	0.3	1.1
o	0.1	1.5	0.3	0.6	4.1	0.4	3.2	1.0	0.1	0.5	0.5	2.7	0.5
n	1.8	3.1	1.5	1.8	0.3	1.0	0.1	1.4	0.3	0.3	3.3	0.3	0.9
i	1.0	2.4	0.5	1.8	4.7	–	0.6	3.0	0.0	1.1	0.4	–	1.5
r	4.1	1.8	1.6	1.5	0.3	2.2	0.5	1.1	0.1	0.3	0.4	0.2	0.4
s	2.4	3.4	4.4	2.0	0.5	1.2	0.5	1.1	0.8	0.2	0.2	0.8	0.6
h	7.0	0.6	2.4	1.3	0.1	2.0	0.2	0.1	0.1	0.1	–	0.1	0.1
l	2.0	0.5	1.0	0.8	–	1.6	–	0.3	–	1.5	0.8	0.2	0.2
d	1.1	1.1	1.3	1.0	0.1	1.6	0.3	0.9	0.1	0.2	0.3	0.2	0.1
u	0.3	1.3	0.5	0.1	0.9	0.1	1.4	1.2	0.1	0.8	0.3	–	0.5
c	1.5	1.1	1.2	1.7	–	0.4	0.2	–	1.3	0.4	–	0.4	0.3

	N	H	U	A	T	O	F	G	Y	C	Z	J	X
N	–	1	5	5	4	–	7	5	–	1	3	–	1
H	3	2	1	1	2	4	–	1	9	1	–	1	–
U	–	1	–	–	4	–	3	2	–	5	1	–	–
A	1	1	–	–	2	–	4	–	–	1	1	1	–
T	1	4	1	–	–	3	3	–	1	–	1	3	1
O	–	4	1	2	7	–	1	4	–	2	–	–	–
F	3	2	2	–	1	1	–	2	1	–	1	–	–
G	4	2	–	2	–	6	–	2	–	–	–	3	–
Y	7	–	–	1	–	3	–	–	–	–	–	1	–
C	2	1	1	–	–	4	–	1	–	–	–	2	–
Z	3	1	–	1	–	–	–	1	–	–	–	1	–
J	–	2	2	–	1	2	2	–	–	1	–	–	3
X	3	–	1	–	–	2	–	–	1	–	–	–	1

Tabelle 18. Erwartungswerte für die Bigrammhäufigkeit und ausgezählte Bigrammhäufigkeiten (nach geeigneter Permutation)

Übereinstimmung der beobachteten Bigrammhäufigkeiten mit den erwarteten ergeben. Auch hier ist maschinelle Durchführung möglich.

15.8.5 Manchmal ist es einfacher, statt den Text zu rekonstruieren, den aus einem Kennwort abgeleiteten Schlüssel (sofern das so ist) zu rekonstruieren. Diese Schlüsselrekonstruktion könnte im obigen Beispiel bereits einsetzen, sobald der Einstieg geschafft ist: Hat man die Zuordnung

U	*	*	*	N	*	*	Y	O	*	*	*	*	T	A	*	*	F	G	H	*	*	*	*	*	*
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

gefunden, so drängt sich auf, von den vier Buchstaben B C D E zwei zwischen A und F einzusortieren, die zwei übrigen zum Aufbau des Kennworts zu nutzen. Von den sechs Fällen führt exhaustiv im weiteren Verlauf zum Erfolg das

Einsortieren von B und D mit der sich ergebenden teilweisen Zuordnung

U	*	*	*	N	E	*	Y	O	*	*	C	*	T	A	B	D	F	G	H	*	*	*	*	*	*
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

— ein zwar spekulatives, aber intellektuell reizvolles Vorgehen.

15.9 Häufigkeitserkennung für polygraphische Substitutionen

Polygraphische Substitutionen kann man wie einfache Substitutionen behandeln, wenn man m-gramme als Einzelzeichen auffaßt. Allerdings bekommt man dann ein umfängliches Alphabet von N^m Zeichen. Von den 676 Bigrammen des normalen Englisch kommen jedoch normalerweise nur rund dreihundert vor (Tabelle 10), von den 17 576 Trigrammen auch nicht viel mehr. Es besteht auch eine ausgeprägte Häufigkeitsverteilung, die einen Einstieg in die unbefugte Entzifferung erleichtert.

15.9.1 Trivial wird die Aufgabe, wenn zwar für die Zeilen- und Spalteneingänge Schlüsselwörter benutzt werden, die Matrix aber die Standardmatrix (vgl. 4.1.2) ist:

	a	m	e	r	i	c	...
e	AA	AB	AC	AD	AE	AF	...
q	BA	BB	BC	BD	BE	BF	...
u	CA	CB	CC	CD	CE	CF	...
a	DA	DB	DC	DD	DE	DF	...
l	EA	EB	EC	ED	EE	EF	...
i	FA	FB	FC	FD	FE	FF	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	

Es handelt sich dann lediglich um eine monographische 2-alphabetische Chiffrierung mit der Periode Zwei (siehe 17. Kapitel).

15.9.2 Ein vor allem bei Amateuren beliebtes, aber neuerdings eher bedeutungsloses polygraphisches Verfahren, PLAYFAIR (vgl. 4.2.1), ist nicht nur in seiner Komplexität sehr eingeschränkt, sondern zeigt auch verborgene Symmetrien: Zu jeder Playfair-Matrix ist jede durch waagrechtes und/oder senkrechtes Abrollen des Torus entstehende Playfair-Matrix äquivalent:

P	A	**L**	**M**	**E**		**L**	**M**	**E**	**P**	A		U	H	**I**	K	Q
R	**S**	T	O	N		T	O	N	R	**S**		Z	V	**W**	X	Y
B	**C**	D	F	G		D	F	G	B	**C**		**E**	**P**	A	**L**	**M**
H	**I**	K	Q	U		K	Q	U	H	**I**		N	R	**S**	T	O
V	**W**	X	Y	Z		X	Y	Z	V	**W**		G	B	**C**	D	F

Bezeichnend für diese Einschränkung ist vor allem, daß für ein Klartextbigramm, das einen Buchstaben X enthält, das Chiffren-Bigramm nur aus zwei von gewissen acht Buchstaben aufgebaut ist, nämlich denen, die in der Zeile von X oder in der Spalte von X stehen. Überdies ist die Chiffre eines revertierten Bigramms oft die Revertierung der Chiffre des Bigramm — immer dann nämlich, wenn ein ‚Überkreuz-Schritt' angewandt wurde.

Die Bigrammhäufigkeiten des Geheimtextes entsprechen denen der Sprache. Die Einzelzeichenhäufigkeiten sind jedoch typischerweise verändert, und zwar dahingehend, daß eine umfänglichere Clique häufigerer Zeichen, und eine umfänglichere Clique seltenerer Zeichen entsteht.

Intuitive Lösungsmethoden für PLAYFAIR basieren auf der Bigrammhäufigkeit in Verbindung mit den eben erwähnten Eigentümlichkeiten, wobei auch wahrscheinliche Wörter herangezogen werden. Sie wurden erstmals systematisch 1916 von Colonel *Parker Hitt*, 1918 von *André Langie* und 1922 von *W. W. Smith* untersucht. PLAYFAIR wurde im 2. Weltkrieg, wo immer es noch eingesetzt wurde, regelmäßig gebrochen; auch dem modifizierten PLAYFAIR (4.2.2), das von den unteren Einheiten des Deutschen Afrikakorps verwendet wurde, ging es nicht besser.

Normalerweise nimmt der unbefugte Entzifferer an, daß er die Phasenlage einer polygraphischen Entzifferung kennt. Das kann ein frommer Wunsch sein: Setzt man vor eine Geheimnachricht in PLAYFAIR eine vereinbarte ungerade Anzahl von Blendern, so ist die Nachricht ‚außer Phase'. Zwar macht es nicht viel aus, zwei Fälle durchzuprobieren, aber der unbefugte Entzifferer muß darauf vorbereitet sein, um sich nicht zu verrennen.

15.10 Freistil-Methoden

Eine klare Trennung der Methoden, wie wir sie vorgenommen haben, dient vor allem dem Verständnis und ist unumgänglich, wenn maschinelle Unterstützung programmiert werden soll. Das Zusammenspiel der so verfügbar gemachten Methoden kann den Wert jeder einzelnen erhöhen. Dieses Zusammenspiel kommt besonders zur Geltung, wenn ein erfahrener Kryptanalyst „von Hand" arbeitet – die Literatur kennt einige einschlägige Berichte, so von *Bazeries*, von *Hitt*, von *Friedman* – oder wenn phantasiebegabte Amateure – bis hin zu *Babbage* – am Werk sind.

15.10.1 Ein besonders hübsches Beispiel ist in die Weltliteratur eingegangen. Im Jahre 1843 schrieb *Edgar Allan Poe* (1809–1849) die Abenteuererzählung "The Gold-Bug", die eine chiffrierte Nachricht und ihre Auflösung enthält. Lustigerweise besteht das Chiffrenalphabet nicht aus Buchstaben, sondern aus Ziffern und sonstigen Lettern, die der Buchdrucker greifbar hat – *Poe* war eben ein ≪*homme de lettres*≫. Der Geheimtext von 203 Zeichen lautet[7]

5 3 ‡ ‡ † 3 0 5)) 6 * ; 4 8 2 6) 4 ‡ .) 4 ‡) ; 8 0 6 * ; 4 8 † 8 ¶
6 0)) 8 5 ; 1 ‡ (; : ‡ * 8 † 8 3 (8 8) 5 * † ; 4 6 (; 8 8 * 9 6 *
? ; 8) * ‡ (; 4 8 5) ; 5 * † 2 : * ‡ (; 4 9 5 6 * 2 (5 * – 4) 8 ¶
8 * ; 4 0 6 9 2 8 5) ;) 6 † 8) 4 ‡ ‡ ; 1 (‡ 9 ; 4 8 0 8 1 ; 8 : 8 ‡

[7] Die zahlreichen Nachdrucke und Übersetzungen von *Poe*s Geschichte strotzen von Setzfehlern in diesen sechs Zeilen. Man sieht, wie schwierig für einen Setzer die Arbeit ist, wenn er keine semantische Rückkontrolle hat.

1 ; 4 8 † 8 5 ; 4) 4 8 5 † 5 2 8 8 0 6 ∗ 8 1 (‡ 9 ; 4 8 ; (8 8 ; 4 (
‡ ? 3 4 ; 4 8) 4 ‡ ; 1 6 1 ; : 1 8 8 ; ‡ ? ;

und *Poe* läßt *Legrand*, den Helden der Geschichte, mit der Bemerkung beginnen, daß es sich wohl um ein System (er nennt es '*cryptograph*') handelt, das den Geisteskräften von Captain *Kidd*, dem Bösewicht der Geschichte, angemessen war, also 'a simple species', nichtsdestoweniger für einfache Matrosen undurchschaubar. *Legrand*, der sich brüstet, viel tausend mal kompliziertere Geheimnachrichten gebrochen zu haben, stellt dann fest, daß nach den geographischen Umständen Französisch oder Spanisch als Sprache in Frage käme, daß aber glücklicherweise die Unterschrift '*Kidd*' klarerweise auf Englisch hindeute. Auch bemerkt er, daß das Fehlen von Wortzwischenräumen (und Interpunktionen) die Aufgabe erschwere. Er stellte deshalb die Einzelzeichen-Häufigkeitstabelle auf, die da ist

33	26	19	16	16	13	12	11	10	8	8	6	5	5	4	4	3	2	1	1
8	;	4	‡	)	∗	5	6	(	†	1	0	9	2	:	3	?	¶	–	.

und beginnt mit der naheliegenden Annahme 8 ≐ e , die durch das häufige Vorkommen des Doppel-e — eine Bigramm-Überlegung — noch gestützt werde. Dann sucht er nach dem häufigsten Trigram /the/ , nämlich nach einem wiederholten Muster mit 8 am Ende. Er findet sieben Vorkommen von ;48 , und nimmt weiterhin an ; ≙ t , 4 ≙ h .

'Thus, a great step has been taken' läßt *Edgar Allan Poe* ihn sagen. Der Einstieg ist bereits gelungen. Die vorletzte Zeile wird zu

1 t h e † e 5 t h) h e 5 † 5 2 e e 0 6 ∗ e 1 (‡ 9 t h e t (e e t h (.

thet(ee gegen Ende der Zeile läßt ihn sofort an (≙ r denken. Das ergibt fortgesetzt thetreethr‡?3hthe und suggeriert /thetreethroughthe/ , also ‡ ≙ o , ? ≙ u , 3 ≙ g . Des weiteren findet er in der zweiten Zeile †83(88, d.h. †egree als /degree/, was † ≙ d mit sich bringt, und vier Zeichen weiter ;46(;88∗, d.h. th6rtee∗ , als /thirteen/, woraus 6 ≙ i und ∗ ≙ n .

Nun sind fast alle der häufigen Zeichen (bis auf a und s) bestimmt. Der teilentzifferte Text lautet jetzt

5 g o o d g 0 5)) i n t h e 2 i) h o .) h o) t e 0 i n t h e d e ¶
i 0)) e 5 t 1 o r t : o n e d e g r e e) 5 n d t h i r t e e n 9 i n
u t e) n o r t h e 5) t 5 n d 2 : n o r t h 9 5 i n 2 r 5 n – h) e ¶
e n t h 0 i 9 2 e 5) t) i d e) h o o t 1 r o 9 t h e 0 e 1 t e : e o
1 t h e d e 5 t h) h e 5 d 5 2 e e 0 i n e 1 r 0 9 t h e t r e e t h r
o u g h t h e) h o t 1 i 1 t : 1 e e t o u t

und man liest heraus

5 ≙ a ,) ≙ s , sowie weiterhin der Reihe nach

0 ≙ l , 2 ≙ b , . ≙ p , ¶ ≙ v , 1 ≙ f , : ≙ y , 9 ≙ m , – ≙ c .

Die Chiffriertabelle lautet

8	;	4	‡	)	*	5	6	(	†	1	0	9	2	:	3	?	¶	–	.	
e	t	h	o	s	n	a	i	r	d	f	l	m	b	y	g	u	v	c	p	

und der Klartext in menschenfreundlicher Form

'*A good glass in the Bishop's hostel in the Devil's seat – forty-one degrees and thirteen minutes – northeast and by north – main branch seventh limb east side – shoot from the left eye of the death's-head – a bee-line from the tree through the shot fifty feet out.*'

Was der Klartext bedeutet, ist allerdings eine Sache für sich; hier muß der Leser zum Original von *Edgar Allan Poe* greifen.

15.10.2 Bezeichnenderweise war kein Wort darüber zu verlieren, ob die Chiffrierung etwa polyalphabetisch sei. *Poe* war monoalphabetisch eingestellt.

15.11 Nochmals: Unizitätslänge

Die Kenntnis der Wahrscheinlichkeit von n-grammen erlaubt auch, zu verstehen, wie bei der Exhaustion in 12.5 das Herauslesen des „richtigen" Klartextes zustande kommt und wieso es eine ‚Unizitätslänge' (12.6) gibt. Eine unwahrscheinliche Buchstabenfolge ist kaum eine „richtige" Nachricht, eine Buchstabenfolge aber, die eine Wahrscheinlichkeit nahe bei Eins besitzt, kann man als „richtige" ansehen. Die Unizitätslänge ist die kleinste Länge des Textes, die für irgendeine Dechiffrierung eine Wahrscheinlichkeit nahe bei Eins (und für alle anderen Dechiffrierungen eine Wahrscheinlichkeit nahe bei Null) zustandebringt.

Das Herauslesen des „richtigen" Klartextes durch einen Menschen ('*running down the list*'), das durch einen optischen und cerebralen Perzeptionsvorgang geschieht, kann durch eine statistische Analyse simuliert werden.

Für das Beispiel von 12.5, Tabelle 5, und zwar beginnend mit der sechsten Spalte, zeigt dies Tabelle 19. Die Wahrscheinlichkeiten sind auf grund der in 15.5.1 erwähnten Textbasis SZ3-92 bestimmt und auf 100% hochgerechnet. Es zeigt sich deutlich, wie schon bei der Länge 3 das SCH 90.5% ausmacht, gefolgt von TDI mit 8.5%, und alle anderen Trigramme bis auf HRW mit 0.45% und vielleicht EOT mit 0.11% und LVA mit 0.11% abgeschlagen sind; bei der Länge 4 kommt EOTA mit 1.27% noch ein wenig hoch; bei der Länge 5 ist für SCHON schon alles klar. Die Unizitätslänge ist in diesem Beispiel 5, wenn nicht gar 4.

Diese Exhaustion hat aber ihre Grenzen, wenn sie in die Zehntausende von Versuchen geht, und scheidet für volle monoalphabetische Substitution aus, wenn keine weitere Information herangezogen werden kann.

"No monoalphabetic substitution can maintain security in heavy traffic."
David Kahn 1967

	Länge 1	Länge 2	Länge 3	Länge 4	Länge 5
V F K R Q	0.76	0.02			
W G L S R	2.03	0.04			
X H M T S	0.01	0.01			
Y I N U T	0.01	0.06	0.06		
Z J O V U	1.21	0.03	0.05		
A K P W V	5.96	1.88	0.01		
B L Q X W	1.77	2.35			
C M R Y X	3.17	0.03			
D N S Z Y	5.22	1.44	0.01		
E O T A Z	17.98	1.58	0.11	1.27	
F P U B A	1.23	0.19	0.03		
G Q V C B	3.25				
H R W D C	4.61	9.54	0.45		
I S X E D	7.97	20.30	0.01		
J T Y F E	0.06				
K U Z G F	1.12	2.34			
L V A H G	3.19	0.71	0.11		
M W B I H	2.47	0.86			
N X C J I	11.06	0.03			
O Y D K J	2.00	0.14	0.01		
P Z E L K	0.59	0.05			
Q A F M L	0.01				
R B G N M	6.42	6.38	0.05		
S C H O N	7.48	22.84	90.51	98.73	100.00
T D I P O	5.55	9.09	8.56		
U E J Q P	4.87	20.09	0.03		
	100.00	100.00	100.00	100.00	100.00

Tabelle 19. Schrittweise Aussiebung der Nachrichten nach der n-gramm-Wahrscheinlichkeit (in %)

16 Kappa und Chi

"Riverbank Publication No. 22,
written in 1920 when Friedman was 28,
must be regarded as the most important
single publication in cryptology."
David Kahn 1967

"The index of coincidence was the most ubiquitous
of the new theoretically justified statistical procedures.
It was a formal and universal method that could not be
made worthless by a slight change in a cipher system."
Colin Burke 1994

Es mag überraschen, daß man von einem vorgelegten monoalphabetisch chiffrierten Text leichter sagen kann, ob er englisch oder französisch ist, als ihn zu entschlüsseln. Dies gilt natürlich auch für Klartext: Es gibt ein einfaches Verfahren, genügend langen Klartext auf Zugehörigkeit zu einer bekannten Sprache zu untersuchen, ohne von ihm „Kenntnis zu nehmen" – ohne seine Syntax und Semantik zu betrachten. Ebenso gibt es ein einfaches Verfahren, um von zwei Texten – ohne sie in Augenschein zu nehmen – zu entscheiden, ob sie in der selben Sprache abgefaßt sind oder nicht.

16.1 Definition und Invarianz von Kappa

Vorgelegt seien zwei Texte $T = (t_1, t_2, t_3, \dots t_M)$, $T' = (t'_1, t'_2, t'_3, \dots t'_M)$ gleicher Länge M über dem selben Zeichenvorrat. Die relative Häufigkeit der zeichenweisen Übereinstimmung in den übereinandergelegten Texten (die **Zeichenkoinzidenz**) soll als das *Kappa* der beiden Texte bezeichnet werden (*W. F. Friedman* 1922, '*index of coincidence*', abgekürzt oft *IC*). Es ist also

$$Kappa(T, T') = \sum_{\mu=1}^{M} \delta(t_\mu, t'_\mu)/M$$

mit der **Indikatorfunktion** (‚Delta-Funktion')

$$\delta(x, y) = \begin{cases} 1 & \text{falls } x = y \\ 0 & \text{sonst} \end{cases} .$$

Beispiel 1 ($M = 180$)

```
T:  e s t a u c h t v o n z e i t z u z e i t i m m e r w i e d e r e i n m
T': u n t e r s c h w e i z e r p o l i t i k e r n w a e c h s t d i e a n
        *                 * *             *

    a l a u f u m k u r z d a r a u f e i l f e r t i g d e m e n t i e r t
    g s t d e n n a e c h s t e n z u g r i c h t u n g e g z u v e r p a s
                                                      *

    z u w e r d e n d a s g e r u e c h t d a s s s i c h d i e o e l e x p
    s e n a u s s e n m i n i s t e r r e n e f e l b e r s a h s i c h j e
                                      *

    o r t i e r e n d e n l a e n d e r v o m d o l l a r l o e s e n w o l
    t z t u e b e r r a s c h e n d e i n e r f o r d e r u n g a u s d e m
        *   *   *             * * * *           *       *

    l e n z u v e r d e n k e n w a e r e e s i h n e n f r e i l i c h n i
    s t a e n d e r a t a u s g e s e t z t e i n b e i t r i t t s g e s u
                * *                 *         *     *     *
```

Beispiel 2 ($M = 180$)

```
T:  t h e p r e c e d i n g c h a p t e r h a s i n d i c a t e d h o w a m
T': w o u l d s e e m t h a t o n e w a y t o o b t a i n g r e a t e r s e
                  *                                   *       *

    o n o a l p h a b e t i c c i p h e r c a n b e s o l v e d e v e n i f
    c u r i t y w o u l d b e t o u s e m o r e t h a n o n e a l p h a b e
                                      *                     *

    t h e o r i g i n a l w o r d l e n g t h s a r e c o n c e a l e d a n
    t i n e n c i p h e r i n g a m e s s a g e t h e g e n e r a l s y s t
    *                               *               *     *     *

    d t h e s u b s t i t u t i o n a l p h a b e t i s r a n d o m i t i s
    e m c o u l d b e o n e t h a t u s e s a n u m b e r o f d i f f e r e
                            *                           *

    p o s s i b l e t o f i n d a s o l u t i o n b y u s i n g f r e q u e
    n t a l p h a b e t s f o r e n c i p h e r m e n t w i t h a n u n d e
                                                          *               *
```

Es ergibt sich in Beispiel 1 $Kappa(T, T') = 21/180 = 11.67\%$; in Beispiel 2 $Kappa(T, T') = 14/180 = 7.78\%$.

16.1.1 Selbstverständlich gilt

$$Kappa(T, T') \leq 1 \;, \quad \text{wobei}$$

$$Kappa(T, T') = 1 \qquad \text{genau dann, wenn } T \doteq T' \;.$$

Empirisch findet man, daß genügend lange Texte aus ein und der selben Sprache S (bzw. des selben Genres dieser Sprache) ziemlich übereinstimmende Werte κ_S von $Kappa(T, T')$ haben, daß sich aber der Wert von Sprache zu Sprache ändert. So findet man folgende Werte für κ_S :

S	N	*Kullback* 1976	*Eyraud* 1953
Englisch	26	6.61%	6.75%
Deutsch	26	7.62%	8.20%
Französisch	26	7.78%	8.00%
Italienisch	26	7.38%	7.54%
Spanisch	26	7.75%	7.69%
Japanisch (Romaji)	26	8.19%	
Russisch	32	5.29%	4.70%

Die Werte in der Literatur streuen noch sehr: 6.5 bis 6.9% für Englisch, 7.5 bis 8.3% für Deutsch. Auf der Basis des in 15.5.1 erwähnten Textmaterials ergibt sich für das Englische ein Wert $\kappa_e = 6.58\%$, für das Deutsche ein Wert $\kappa_d = 7.62\%$, in guter Übereinstimmung mit den Werten von *Kullback*.

Die Werte für κ_S, das empirische *Kappa* einer Sprache S, spiegeln etwas die Redundanz der Sprachen wider: Die Übersetzung des Markus-Evangeliums, die im Englischen 29 000 Silben hat, hat (nach *Mencken*) in den germanischen Sprachen im Mittel 32 650 Silben, in den romanischen Sprachen im Mittel 40 200 Silben, in den slawischen Sprachen im Mittel 36 500 Silben. Aber es besteht kein strenger Zusammenhang.

16.1.2 Evidenterweise hat man

Invarianzsatz 5: Für alle *polyalphabetischen*, funktionalen monographischen Chiffrierungen, insbesondere für alle linearen *polyalphabetischen* monographischen Chiffrierungen gilt:
Das Kappa zweier (gleichlanger) Texte, die mit dem gleichen Schlüssel chiffriert werden, bleibt erhalten.

Invarianzsatz 6: Für alle Transpositionen gilt:
Das Kappa zweier (gleichlanger) Texte, die mit dem gleichen Schlüssel chiffriert werden, bleibt erhalten.

Soweit das *Kappa* also für eine in Frage kommende Sprache kennzeichnend ist, läßt sich die Sprache aus dem Chiffrat erkennen.

16.1.3 Der Erwartungswert für das *Kappa* zweier Texte (mit gleichem Alphabet) errechnet sich aus den Wahrscheinlichkeiten p_i, p'_i des Auftretens der Zeichen in den ‚stochastischen Quellen' Q, Q' der Sprachen: Der Erwartungswert für das Auftreten des Zeichens χ_i an der μ-ten Stelle beider Texte ist $p_i \cdot p'_i$; es ergibt sich der Erwartungswert für $Kappa(T,T')$

$$\langle Kappa(T,T')\rangle_{QQ'} = \sum_{i=1}^{N} p_i \cdot p'_i \ .$$

Sind beide Quellen identisch, $Q' = Q$, so ist $p'_i = p_i$ und

$$(*) \qquad \langle Kappa(T,T')\rangle_{Q} = \sum_{i=1}^{N} p_i^2 \ .$$

Diese Gleichung setzt die Definition von *Kappa* in Beziehung zum klassischen Urnenexperiment der Wahrscheinlichkeitstheorie.

Satz: Für identische Quellen $Q' = Q$ gilt

$$\frac{1}{N} \leq \langle Kappa(T,T') \rangle_Q \leq 1 \ ,$$

wobei die linke Grenze angenommen wird für den Fall der Gleichverteilung $Q_{\mathrm{R}} : p_i = \frac{1}{N}$, und nur dafür; die rechte für jede deterministische Verteilung $Q_j : p_j = 1, \, p_i = 0$ für $i \neq j$, und für keine andere Verteilung.

Aus der in 15.5.3, Tabelle 8 postulierten Wahrscheinlichkeitsverteilung ergibt sich, wie schon gesagt

$$\langle Kappa(T,T') \rangle_{\mathrm{Deutsch}} = 0.07619 = \kappa_{\mathrm{d}} \ ,$$

$$\langle Kappa(T,T') \rangle_{\mathrm{Englisch}} = 0.06577 = \kappa_{\mathrm{e}} \ .$$

Für die Quelle mit Gleichverteilung Q_{R} erhält man ($N = 26$)

$$\langle Kappa(T,T') \rangle_{\mathrm{R}} = \kappa_{\mathrm{R}} = 0.03846 = \frac{1}{26} \ .$$

Der *Kappa*-Test unterscheidet also deutsche und englische Quellen deutlich von einer gleichverteilten Quelle. Als Faustregel für die gängigen Sprachen mag gelten:

Das Verhältnis $\langle Kappa(T,T') \rangle_{\mathrm{S}} / \langle Kappa(T,T') \rangle_{\mathrm{R}}$ *liegt nahe bei 2.*

Es ist

$$\kappa_{\mathrm{d}} / \kappa_{\mathrm{R}} = N \cdot \kappa_{\mathrm{d}} = 1.98 \ , \quad \kappa_{\mathrm{e}} / \kappa_{\mathrm{R}} = N \cdot \kappa_{\mathrm{e}} = 1.71 \ .$$

16.2 Definition und Invarianz von Chi und Psi

Vorgelegt seien wieder zwei Texte gleicher Länge M über dem selben Zeichenvorrat von N Zeichen, $T = (t_1, t_2, t_3, \ldots t_M)$, $T' = (t'_1, t'_2, t'_3, \ldots t'_M)$.

Die Häufigkeit des Vorkommens des Zeichens χ_i im Text T sei mit m_i, im Text T' mit m'_i bezeichnet. Es ist

$$\textstyle\sum_{i=1}^N m_i = M \ , \quad \sum_{i=1}^N m'_i = M \ .$$

Als *Chi* wird bezeichnet die '*cross-product sum*' (*Solomon Kullback*, 1935)

$$Chi(T,T') = (\textstyle\sum_{i=1}^N m_i \cdot m'_i)/M^2 \ .$$

Homogen geschrieben, lautet die Definition

$$Chi(T,T') = (\textstyle\sum_{i=1}^N m_i \cdot m'_i)/(\ (\sum_{i=1}^N m_i) \cdot (\sum_{i=1}^N m'_i) \ ) \ .$$

Die beiden Texte von 16.1, Beispiel 1 haben folgende Häufigkeiten

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
T	10	0	4	11	35	4	2	5	15	0	2	10	6	14	7	1	0	15	7	9	9	3	4	1	0	6
T'	11	3	6	6	33	2	7	7	12	1	1	2	2	16	2	2	0	15	18	16	10	1	2	0	0	5

Damit ergibt sich $\quad Chi(T,T') = \frac{2492}{180 \cdot 180} = 7.69\% \ .$

Für die beiden Texte von 16.1, Beispiel 2 erhält man

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
T	15	6	8	9	21	3	4	10	17	0	0	8	2	14	12	6	1	8	11	14	5	2	2	0	1	0
T'	15	6	4	5	30	4	4	9	8	0	0	6	6	15	12	4	0	10	10	17	8	0	4	0	3	0

Damit ergibt sich $\quad Chi(T,T') = \frac{2139}{180 \cdot 180} = 6.60\%$.

16.2.1 Ähnlich wie in 16.1.1 gilt auch

$$Chi(T,T') \leq 1 , \quad \text{wobei}$$

$Chi(T,T') = 1$ genau dann, wenn T und T' aus einem einzigen Zeichen aufgebaut sind.

Dies folgt aus elementaren geometrischen Überlegungen.

Sind alle m_i gleich, $m_i = M/N$, so ist (bei beliebigen m'_i)

$$Chi(T,T') = \tfrac{1}{N} = \kappa_{\mathrm{R}} .$$

Empirisch findet man wieder, daß genügend lange Texte aus ein und der selben Sprache S (bzw. des selben Genres dieser Sprache) nicht nur ziemlich übereinstimmende (von Sprache zu Sprache sich ändernde) Werte von *Chi* haben, sondern daß diese Werte bei den entsprechenden Werten von *Kappa* liegen. Dies wird sich in 16.3. aufklären.

16.2.2 Wichtig ist jetzt der Spezialfall $T' = T$, $m'_i = m_i$. Sei

$$Psi(T) = Chi(T,T) = \textstyle\sum_{i=1}^{N} m_i^2/M^2 .$$

Es gilt der Steinersche Satz

$$\sum_{i=1}^{N}(m_i - \frac{M}{N})^2/M^2 = \sum_{i=1}^{N} m_i^2/M^2 - \frac{1}{N} .$$

Somit gilt

$$\tfrac{1}{N} \leq Psi(T) \leq 1 , \quad \text{wobei}^{1}$$

$Psi(T) = \frac{1}{N} = \kappa_{\mathrm{R}}$ genau dann, wenn alle m_i gleich sind,

$Psi(T) = 1$ genau dann, wenn T aus einem einzigen Zeichen aufgebaut ist.

16.2.3 Auch *Chi* und *Psi* haben Invarianzeigenschaften. Nunmehr gilt jedoch gegenüber *Kappa* nur noch eine schwächere Aussage:

---

[1] Für den extremen Fall $M < N$ gilt schärfer $\frac{1}{M} \leq Psi(T)$, wobei $Psi(T) = \frac{1}{M}$ genau dann, wenn $m_i \in \{0,1\}$.

Invarianzsatz 7: Für alle *monoalphabetischen*, funktionalen monographischen Substitutionen, insbesondere auch für alle linearen *monoalphabetischen* monographischen Substitutionen gilt:
Das Chi zweier (gleichlanger) Texte, die gleichartig chiffriert werden, wie auch das Psi eines Textes, bleiben erhalten.

Invarianzsatz 8: Für alle Transpositionen gilt:
Das Chi zweier (gleichlanger) Texte, die gleichartig chiffriert werden, wie auch das Psi eines Textes, bleiben erhalten.

Soweit das *Chi* bzw. *Psi* also für eine in Frage kommende Sprache kennzeichnend ist, läßt sich die Sprache aus dem Chiffrat erkennen.

16.2.4 Der Erwartungswert für das *Chi* zweier Sprachen (mit gleichem Alphabet) errechnet sich direkt aus den Wahrscheinlichkeiten p_i, p'_i des Auftretens der Zeichen in den ‚stochastischen Quellen' Q, Q' der Sprachen: Der Erwartungswert für die Anzahl der Zeichens χ_i ist $p_i \cdot M$ bzw. $p'_i \cdot M$; es ergibt sich der Erwartungswert für $Chi(T,T')$

$$\langle Chi(T,T')\rangle_{QQ'} = \sum_{i=1}^{N} p_i \cdot p'_i \ .$$

Sind beide Quellen identisch, $p'_i = p_i$, so ist

$$(*) \quad \langle Chi(T,T')\rangle_{Q} = \sum_{i=1}^{N} p_i^2 \ .$$

Insbesondere gilt

$$\langle Psi(T)\rangle_{Q} = \sum_{i=1}^{N} p_i^2 \ .$$

Satz: Für identische Quellen $Q' = Q$ gilt

$$\tfrac{1}{N} \leq \langle Chi(T,T')\rangle_{Q} \leq 1 \ ,$$

und speziell

$$\tfrac{1}{N} \leq \langle Psi(T)\rangle_{Q} \leq 1 \ ,$$

wobei die linke Grenze angenommen wird für den Fall der Gleichverteilung $Q_R : p_i = \frac{1}{N} = \kappa_R$, und nur dafür; die rechte für jede deterministische Verteilung $Q_j : p_j = 1, \ p_i = 0$ für alle $i \neq j$, und für keine andere Verteilung.

Überrascht stellt man fest, daß die mit (∗) gekennzeichneten Erwartungswerte $\langle Kappa(T,T')\rangle_Q$ (vgl. 16.1.3) und $\langle Chi(T,T')\rangle_Q$ zusammenfallen. Es wird sich herausstellen, daß sogar zwischen $Kappa(T,T')$ und $Chi(T,T')$ ein Zusammenhang besteht.

16.3 Das Kappa-Chi-Theorem

Wir benötigen für das folgende zwei Hilfsfunktionen $g_{i,\mu}$, $g'_{i,\mu}$.

Sei $g_{i,\mu} = \begin{cases} 1 & \text{falls } t_\mu \text{, das } \mu\text{-te Zeichen von } T = \chi_i \\ 0 & \text{sonst} \end{cases}$;

entsprechend sei $g'_{i,\mu}$ für T' definiert. Dann ist

$\delta(t_\mu, t'_\nu) = \sum_{i=1}^{N} g_{i,\mu} \cdot g'_{i,\nu}$ und

$m_i = \sum_{\mu=1}^{M} g_{i,\mu}$, $m'_i = \sum_{\nu=1}^{M} g'_{i,\nu}$.

16.3.1 Sei $T^{(r)}$ der um r Plätze nach rechts zyklisch verschobene Text T. Dann ist die Anzahl Koinzidenzen zwischen $T^{(r)}$ und T'

$Kappa(T^{(r)}, T') = \sum_{\mu=1}^{M} \delta(t_{(\mu-r-1) \bmod M+1}, t'_\mu)/M$.

Speziell ist $Kappa(T^{(0)}, T') = Kappa(T, T')$.

16.3.2 Wir formulieren nun das *Kappa-Chi*-**Theorem**:

$$\frac{1}{M} \sum_{\rho=0}^{M-1} Kappa(T^{(\rho)}, T') = Chi(T, T') .$$

$Chi(T, T')$ ist also das arithmetische Mittel aller $Kappa(T^{(r)}, T')$.

Korollar :
$$\frac{1}{M} \sum_{\rho=0}^{M-1} Kappa(T^{(\rho)}, T) = Psi(T) .$$

Beweis:

$\frac{1}{M} \sum_{\rho=0}^{M-1} Kappa(T^{(\rho)}, T') =$

$\frac{1}{M} \cdot \frac{1}{M} \cdot \sum_{\rho=0}^{M-1} \sum_{\mu=1}^{M} \delta(t_{(\mu-\rho-1) \bmod M+1}, t'_\mu) =$

$\frac{1}{M} \cdot \frac{1}{M} \cdot \sum_{\nu=1}^{M} \sum_{\mu=1}^{M} \delta(t_\mu, t'_\nu) =$

$\frac{1}{M} \cdot \frac{1}{M} \cdot \sum_{\nu=1}^{M} \sum_{\mu=1}^{M} \sum_{i=1}^{N} g_{i,\mu} \cdot g'_{i,\nu} =$

$\frac{1}{M} \cdot \frac{1}{M} \cdot \sum_{i=1}^{N} \sum_{\nu=1}^{M} \sum_{\mu=1}^{M} g_{i,\mu} \cdot g'_{i,\nu} =$

$\frac{1}{M} \cdot \frac{1}{M} \cdot \sum_{i=1}^{N} (\sum_{\nu=1}^{M} g'_{i,\nu}) \cdot (\sum_{\mu=1}^{M} g_{i,\mu}) =$

$\frac{1}{M} \cdot \frac{1}{M} \cdot \sum_{i=1}^{N} m'_i \cdot m_i =$

$Chi(T, T')$.

Es zeigt sich jetzt, daß für die Beispiele 1 und 2 in 16.1 die Werte für *Kappa* mit 11.67% bzw. 7.78% gegenüber den Mittelwerten 7.69% bzw. 6.60% in 16.2 (zufällig) sehr hoch ausgefallen sind.

16.4 Das Kappa-Phi-Theorem

Der Fall $T' = T$ bietet die Besonderheit, daß $Kappa(T^{(0)}, T) = Kappa(T, T) = 1$ nach (16.1.1). Dagegen ist für $r \neq 0$ mit einem bedeutend kleineren Wert von $Kappa(T^{(r)}, T)$ zu rechnen. Somit fällt bei der Mittelbildung der Fall $r = 0$ systematisch aus dem Rahmen, und es empfiehlt sich, eine Mittelbildung nur über die verbleibenden $M - 1$ Werte zu betrachten, nämlich

$$\frac{1}{M-1} \sum_{\rho=1}^{M-1} Kappa(T^{(\rho)}, T) \ .$$

16.4.1 Nun ist
$\frac{1}{M-1} \cdot \sum_{\rho=1}^{M-1} Kappa(T^{(\rho)}, T) =$
$\frac{1}{M-1} \cdot (\sum_{\rho=0}^{M-1} Kappa(T^{(\rho)}, T) - 1) = \frac{1}{M-1} \cdot (M \cdot Psi(T) \ - 1) =$
$\frac{1}{M-1} \cdot (\sum_{i=1}^{N} (m_i^2/M \ - 1)) =$
$\frac{1}{M-1} \cdot \frac{1}{M} \cdot (\sum_{i=1}^{N} (m_i^2 \ - M)) =$
$\frac{1}{M-1} \cdot \frac{1}{M} \cdot (\sum_{i=1}^{N} (m_i^2 \ - m_i)) =$
$\frac{1}{M-1} \cdot \frac{1}{M} \cdot (\sum_{i=1}^{N} m_i \cdot (m_i - 1))$.
Wir definieren also eine neue Größe

$$Phi(T) = (\sum_{i=1}^{N} m_i \cdot (m_i - 1))/(M \cdot (M-1))$$

und haben das *Kappa*-*Phi*-**Theorem**:

$$\frac{1}{M-1} \sum_{\rho=1}^{M-1} Kappa(T^{(\rho)}, T)) = Phi(T) \ .$$

Die Berechnung von $Phi(T)$ hat gegenüber der von $Psi(T)$ den kleinen Vorteil, daß sowohl für den Fall $m_i = 0$ wie für den Fall $m_i = 1$ kein Beitrag zur Summe anfällt,[2] was bei kurzen Texten für die seltenen Buchstaben vorteilhaft ist. Die Literatur arbeitet jedoch nicht nur deshalb überwiegend mit *Phi* statt mit *Psi*, sondern auch weil der *Phi*-Test (neben dem *Chi*-Test) von *Kullback* zuerst auf der Basis entsprechender Überlegungen aus der Stochastik angegeben wurde.

Beispiel 3: Für den Geheimtext T ($M = 280$) von 15.8.1 ergibt sich mit den dort angegebenen Einzelzeichenhäufigkeiten
$280^2 \cdot Psi(T) = 289+16+169+0+49+289+ 529+676+25+144+9+4+4+ 1296+625+1+25+0+0+529+400+9+36+81+169+64 = 5438$,
$280 \cdot 279 \cdot Phi(T) = 272+12+156+0+42+272+ 506+650+20+132+6+2+2+ 1260+600+0+20+0+0+506+380+6+30+72+156+56 = 5158$, also
$Psi(T) = 5438/78400 = 6.936\%$; $Phi(T) = 5158/78120 = 6.603\%$.
Übrigens ergibt sich für Paarhäufigkeiten, also für den Text $T \times T^{(1)}$
$Psi(T \times T^{(1)}) = 871/77841 = 1.119\%$; $Phi(T \times T^{(1)}) = 592/77562 = 0.763\%$.

[2] Es ist $Phi(T) = 0$ genau dann, wenn $m_i \in \{0, 1\}$.

16.4.2 *Phi*(T) ist von *Psi*(T) nicht sehr verschieden: Es ist

$Psi(T) = \frac{M-1}{M} Phi(T) + \frac{1}{M}$, $\quad Phi(T) = \frac{M}{M-1} Psi(T) - \frac{1}{M-1}$ und

$Psi(T) - Phi(T) = \frac{1-Phi(T)}{M} = \frac{1-Psi(T)}{M-1}$, also $Phi(T) \leq Psi(T)$.

16.4.3 *Phi* hat die gleichen Invarianzeigenschaften wie *Psi*:

Invarianzsatz 7bis: Für alle *monoalphabetischen*, funktionalen monographischen Substitutionen, insbesondere auch für alle linearen *monoalphabetischen* monographischen Substitutionen gilt:
Das Phi eines Textes bleibt erhalten.

Invarianzsatz 8bis: Für alle Transpositionen gilt:
Das Phi eines Textes bleibt erhalten.

16.4.4 Der Erwartungswert für das *Phi* eines Textes T der Länge M errechnet sich ebenfalls aus der Wahrscheinlichkeit p_i des Auftretens der Zeichen in der ‚stochastischen Quelle' Q der Sprache: Er ergibt sich zu

$\langle Phi(T)\rangle_Q^{(M)} = \frac{M}{M-1} \cdot (\sum_{i=1}^N p_i \cdot (p_i - \frac{1}{M}))$, wobei

$$\langle Phi(T)\rangle_Q^{(M)} \geq \begin{cases} \frac{M}{M-1} \cdot (\frac{1}{N} - \frac{1}{M}) = \frac{1}{N} \cdot \frac{M-N}{M-1} & \text{falls } M > N \\ 0 & \text{falls } M \leq N \end{cases} .$$

Für größer und größer werdendes M nähert sich der Erwartungswert für *Phi*(T) dem Erwartungswert für *Psi*(T), nämlich

$$\langle Phi(T)\rangle_Q^{(\infty)} = \sum_{i=1}^N p_i^2 .$$

16.5 Symmetrische Funktionen der Zeichenhäufigkeiten

Die Invarianz von *Psi* in Satz 7 und 8 gilt für alle symmetrischen Funktionen der Zeichenhäufigkeiten. Die einfachste nichtkonstante polynomiale Funktion ist in der Tat $\sum_{i=1}^N m_i^2$. Eine interessante Klasse ist die folgende:

$$Psi_a(T) = \begin{cases} (\sum_{i=1}^N (m_i/M)^a)^{1/(a-1)} & \text{falls } 1 < a < \infty \\ \exp(\sum_{i=1}^N (m_i/M) \cdot \ln(m_i/M)) & \text{falls } a = 1 \\ \max_{i=1}^N (m_i/M) & \text{falls } a = \infty \end{cases}$$

mit der Normierung $\sum_{i=1}^N (m_i/M) = 1$. Psi_2 ist *Psi* von oben.
Es gilt für $1 \leq a \leq \infty$ (vgl. 16.2.2)

$Psi_a(T) = \frac{1}{N}$ genau dann, wenn alle m_i gleich sind.

Psi_1 und Psi_∞ sind stetige Grenzfunktionen der Klasse; es ist auch

$Psi_1(T) = \prod_{i=1}^N (m_i/M)^{m_i/M}$.

Die Größe $-\text{ld}\, Psi_a(T)$ heißt **Rényi-a-Entropie** von T (*Rényi*, 1960)[3] ; man erhält

---

[3] *Alfréd Rényi* (1921–1976), ungarischer Mathematiker.

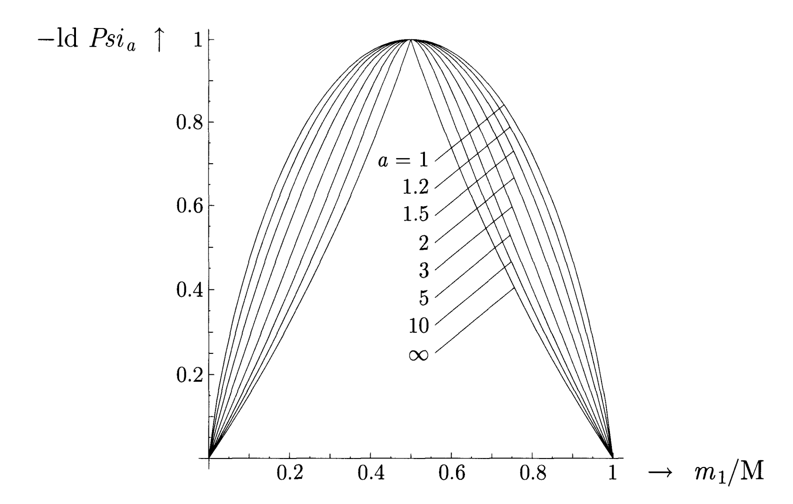


Abb. 114. Verlauf der *Renyi-a*-Entropie für $N = 2$

$$-\mathrm{ld}\, Psi_a(T) = \begin{cases} -\frac{1}{a-1} \cdot \mathrm{ld}\,(\sum_{i=1}^{N}(m_i/M)^a) & \text{falls } 1 < a < \infty \\ -(\sum_{i=1}^{N}(m_i/M) \cdot \mathrm{ld}\,(m_i/M)) & \text{falls } a = 1 \\ -\max_{i=1}^{N} \mathrm{ld}\,(m_i/M) & \text{falls } a = \infty \end{cases}$$

Die Rényi-1-Entropie $-\mathrm{ld}\, Psi_1$ ist die **Shannon-Entropie** (*Claude E. Shannon*, 1945)[4]. Die Rényi-2-Entropie $-\mathrm{ld}\, Psi_2$ könnte man als **Kullback-Entropie** bezeichnen. Abb. 114 zeigt den Verlauf von $-\mathrm{ld}\, Psi_a$ für $N = 2$ und für einige Werte von a .

Für den englischen Text T ($M = 280$) von 15.8.1 ergibt sich

$$\begin{array}{llll} Psi_1(T) & = 5.852\% & -\mathrm{ld}\, Psi_1(T) & = 4.095 \\ Psi_2(T) & = 6.936\% & -\mathrm{ld}\, Psi_2(T) & = 3.850 \ \text{(vgl. 16.4.1)} \\ Psi_\infty(T) & = 12.857\% & -\mathrm{ld}\, Psi_\infty(T) & = 2.959\ . \end{array}$$

Für Zeichenpaare sinken die vergleichbaren Entropie-Werte etwas ab,

$$\begin{array}{llll} \sqrt{Psi_1(T \times T^{(1)})} & = 9.37\% & -\frac{1}{2}\mathrm{ld}\, Psi_1(T \times T^{(1)}) & = 3.42 \\ \sqrt{Psi_2(T \times T^{(1)})} & = 10.58\% & -\frac{1}{2}\mathrm{ld}\, Psi_2(T \times T^{(1)}) & = 3.24 \ \text{(vgl. 16.4.1)} \\ \sqrt{Psi_\infty(T \times T^{(1)})} & = 17.96\% & -\frac{1}{2}\mathrm{ld}\, Psi_\infty(T \times T^{(1)}) & = 2.48\ . \end{array}$$

[4] *Claude E. Shannon* (∗ 1916), amerikanischer Mathematiker, Ingenieur und Informatiker. *Shannon* arbeitete 1936–1938 unter *Vannevar Bush* an der Analogrechner-Entwicklung, wobei er mit Relaisschaltungen zu tun bekam. Dabei entstand 1937 eine wichtige Publikation über den Zusammenhang zwischen Schaltalgebra und Boolescher Algebra: A Symbolic Analysis of Relay and Switching Circuits. Trans. AIEE 57, 713–723 (1938). *Shannon* ging 1941 in die Bell Laboratories, wo er mit mathematischen Fragen der Übermittlung geheimer und verrauschter Nachrichten befaßt wurde. Daraus entstand die Informationstheorie (A Mathematical Theory of Communication, Bell System Technical Journal July 1948, p. 379, Oct. 1948, p. 623), publiziert 1949 zusammen mit *Warren Weaver* (∗ 1923): Mathematical Theory of Communication. Univ. of Illinois Press, Urbana 1949. *Shannon* wurde später Professor am MIT, Cambridge, Mass.

17 Periodenanalyse

"It may be laid down as a principle that it is never worth the trouble of trying any inscrutable cypher unless its author has himself deciphered some very difficult cypher."

Charles Babbage 1854

"The Babbage rule would have deprived cryptologists of some of the most important features of modern cryptography, such as the Vernam mechanism, the rotor, the Hagelin machine."

David Kahn 1967

Periodische polyalphabetische Chiffrierung (2.3.6) enthält trotz einer Fülle möglicherweise unabhängiger Alphabete *ein* Element, das schwer zu verstecken ist: die Periode der Chiffrierung. Dies beruht auf dem folgenden trivialen Sachverhalt: Stammt ein Text P der Länge M aus einer stochastischen Quelle Q, so stammt der um s Plätze zyklisch verschobene Text $P^{(s)}$ aus der selben Quelle.

Sei p_i die Wahrscheinlichkeit des Auftretens des i-ten Zeichens in Q. Es gilt

Satz 1: Ist d die Periode einer periodischen polyalphabetischen funktionalen, einfachen und monopartiten Chiffrierung (der Einfachheit halber sei $d|M$ angenommen), so stammen sowohl das Chiffrat C eines Textes P als auch $C^{(k\cdot d)}$, das um $k\cdot d$ Plätze zyklisch verschobene Chiffrat C, aus der selben stochastischen Quelle Q; es ist für alle k

$$\langle Kappa(C^{(k\cdot d)}, C)\rangle_Q = \sum_{i=1}^{N} p_i^2 \ .$$

Beweis: $P^{(k\cdot d)}$ und P sind aus der selben Quelle und werden der selben polyalphabetischen Chiffrierung unterworfen. Das Chiffrat von $P^{(k\cdot d)}$ stimmt überein mit $C^{(k\cdot d)}$, dem um $k\cdot d$ Plätze zyklisch verschobenen Chiffrat C von P. Nach 16.1.3.(∗) ist $\langle Kappa(C^{(k\cdot d)}, C)\rangle_Q = \langle Kappa(P^{(k\cdot d)}, P)\rangle_Q = \sum_{i=1}^{N} p_i^2$ für beliebiges k.

Hingegen kann man über $\langle Kappa(C^{(u)}, C)\rangle_{Q',Q}$, wo u kein Vielfaches von d ist, eine solche Aussage nicht machen. Denn $C^{(u)}$ und C stammen in der Regel aus voneinander unabhängigen stochastischen Quellen Q' und Q'';

$$\langle Kappa(C^{(u)}, C)\rangle_{Q',Q''} = \sum_{i=1}^{N} p'_i \cdot p''_i \ \text{ fluktuiert um } \frac{1}{N} \ .$$

Dies ist zumindest so, wenn die einzelnen Alphabete eine genügend gründliche Durchmischung der Zeichenhäufigkeiten bewirken und genügend viele Alphabete ins Spiel gebracht werden.

G E I E I	A S G D X	V Z I J Q	L M W L A	A M X Z Y	Z M L W H
F Z E K E	J L V D X	W K W K E	T X L B R	A T Q H L	B M X A A
N U B A I	V S M U K	H S S P W	N V L W K	A G H G N	U M K W D
L N R W E	Q J N X X	V V O A E	G E U W B	Z W M Q Y	M O M L W
X N B X M	W A L P N	F D C F P	X H W Z K	E X H S S	F X K I Y
A H U L M	K N U M Y	E X D M W	B X Z S B	C H V W Z	X P H W L
G N A M I	U K				

Abb. 115. Geheimtext von *G. W. Kulp*

17.1 Friedmans Periodenbestimmung durch Kappa-Test

17.1.1 Für den in Abb. 115 aufgeführten Geheimtext ergibt sich, *Friedman* folgend, der in Abb. 116 aufgezeichnete Verlauf von $Kappa(C^{(u)}, C)$ in Abhängigkeit von u (für $u = 0$ ergibt sich der Wert 1, der außerhalb des Rahmens liegt).

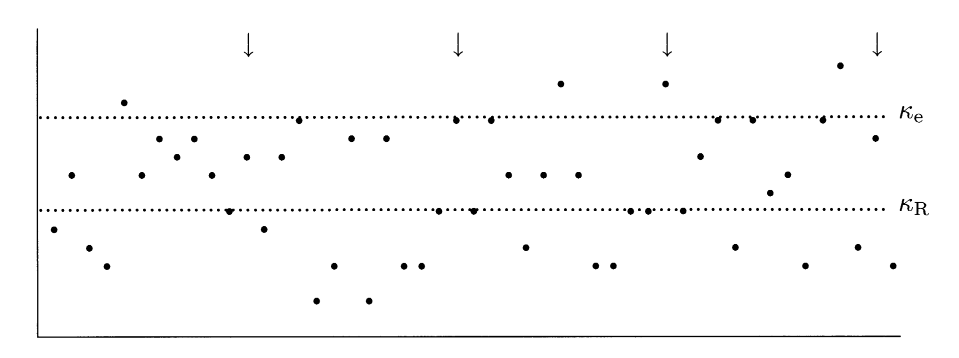


Abb. 116. Kappa-Verlauf für den (englischen) Geheimtext von *G. W. Kulp*

17.1.2 Der Geheimtext von Abb. 115 hat eine Geschichte. Er wurde von einem gewissen *G. W. Kulp* einer Wochenzeitung in Philadelphia, *Alexander's Weekly Messenger*, eingesandt, in der *Edgar Allan Poe* eine Kolumne redigierte, und erschien am 26. Februar 1840 im Druck – mit Worttrennungen und Interpunktionszeichen (Abb. 118). *Poe* hatte monoalphabetisch chiffrierte Geheimtexte erbeten, und „bewies" in einer anschließenden Nummer der Zeitschrift, daß das angebliche Chiffrat ein Schwindel war – *"a jargon of random characters having no meaning whatsoever"*. Er hatte nicht so unrecht – eine Häufigkeitszählung ergibt die in Abb. 117 verzeichneten, ziemlich gleichverteilten Werte. Eine Häufigkeitsbetrachtung konnte nicht zum Erfolg führen.

12	7	2	5	10	4	6	9	6	3	10	12	14	9	2	4	4	2	7	2	7	7	16	15	4	8
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Abb. 117. Häufigkeitsverteilung im Geheimtext von *G. W. Kulp*

Allerdings wären Worttrennungen und Interpunktionen eine große Hilfe für die Mustererkennungsmethode gewesen. Möglicherweise hat *Poe* sie auch versucht und Schiffbruch erlitten und darauf seine apodiktische Feststellung gegründet.

"Ge Jeasgdxv,
Zij gl mw, laam, xzy zmlwhfzek
ejlvdxw kwke tx lbr atgh lbmx aanu
bai Vsmukkss pwn vlwk agh gnumk
wdlnzweg jnbxvv oaeg enwb zwmgy
mo mlw wnbx mw al pnfdcfpkh wzkex
hssf xkiyahul. Mk num yexdm wbxy
sbc hv wyx Phwkgnamcuk?"

Abb. 118. Faksimile des Geheimtextes von *G. W. Kulp* (1840).
Der Setzer hat, wie man später herausgefunden hat, für etliche Druckfehler gesorgt, z.B. q als g gelesen und auch einen Buchstaben ganz unterschlagen.

17.1.3 Die Häufigkeitsverteilung für den Geheimtext von *Kulp* ergibt einen Wert von $\frac{1586}{187 \cdot 186} = 4.56\%$ für *Phi*, bzw. von $\frac{1773}{187^2} = 5.07\%$ für *Psi*. Monoalphabetische Substitution hätte für die zu vermutende englische Sprache bedeutend höhere Werte erbracht; *Psi* liegt näher bei $\kappa_R = \frac{1}{N}$ als bei κ_e . *Kulp* hatte demnach wohl die Bedingung, nur monoalphabetische einfache Substitutionen zu verwenden, nicht eingehalten. Für *Poe* wäre also auch eine monoalphabetische Bigrammsubstitution nicht in Frage gekommen; auch PLAYFAIR nicht, denn PLAYFAIR wurde erst 1854 erfunden.

17.1.4 Abb. 116 zeigt, daß sich einige Kappa-Werte deutlich in der Nähe von κ_e befinden, die meisten aber über oder auch unter κ_R. Bei kleinen Werten von u sind die Kappa-Werte noch durch die Fernwirkung der Muster beeinflußt. Ist ein hoher Wert durch eine Periode begründet, so müssen auch für alle Vielfachen dieser Periode hohe Kappa-Werte auftreten. Damit scheiden die kleinen Zahlen wie 5 für die Periode aus, während 12 ein guter Kandidat ist. 15 kommt wohl nicht in Frage, da für 45 ein sehr niedriger Kappa-Wert kommt. Es ist also zunächst nur eine aussichtsreiche Hypothese, für den Geheimtext von *Kulp* monographische polyalphabetische Chiffrierung mit einer Periode Zwölf zu unterstellen.

Der Geheimtext von *Kulp* ist mit 187 Zeichen recht kurz, so daß beträchtliche Schwankungen der Kappa-Werte zu erwarten sind; für längere Texte heben sich die Periodenvielfachen sehr viel besser ab. Dies zeigt ein Vergleich mit Abb. 119 für einen Text von 300 Zeichen und Abb. 120 für einen Text von 3 000 Zeichen, bei dem die Periode ins Auge springt.

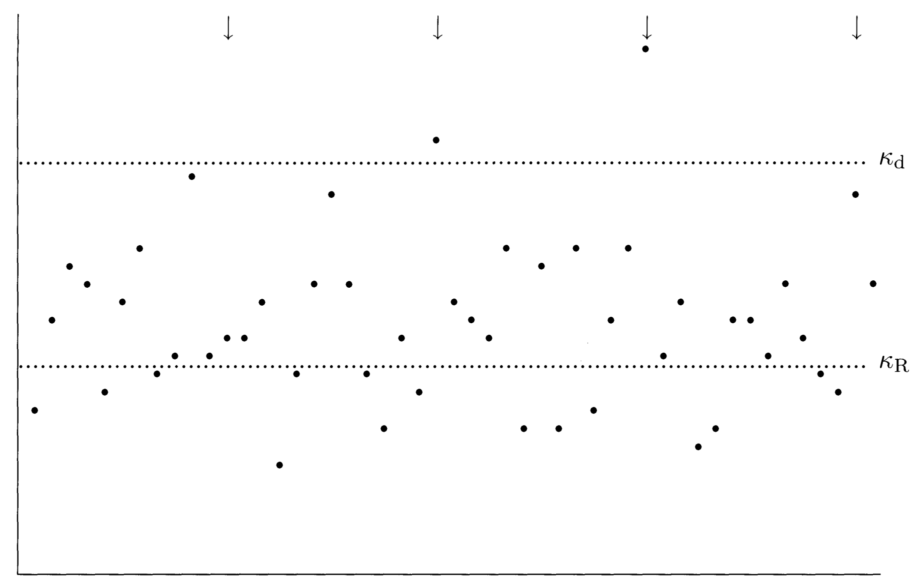


Abb. 119. Kappa-Verlauf für einen (deutschen) Text von 300 Zeichen

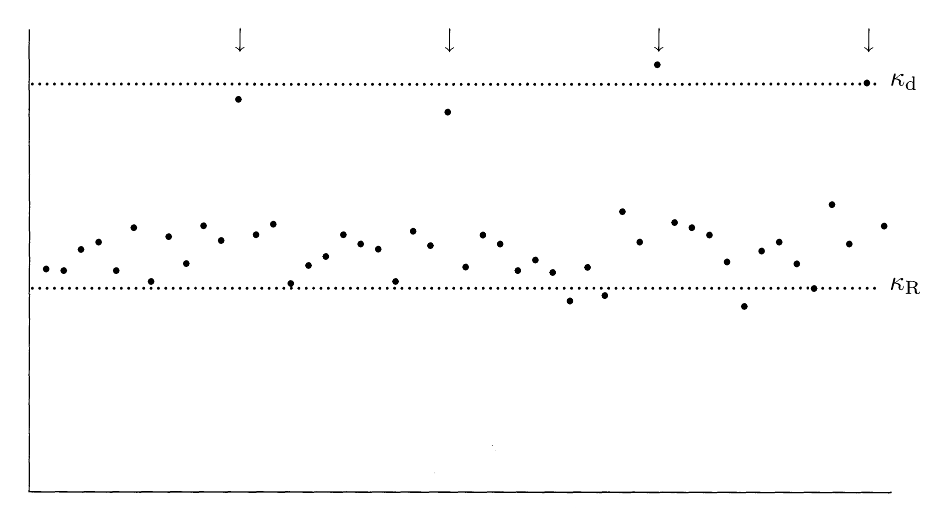


Abb. 120. Kappa-Verlauf für einen (deutschen) Text von 3 000 Zeichen

17.2 Kappa-Test für Multigramme

Die Diskussion braucht jedoch nicht auf Einzelzeichen beschränkt zu werden. Bigramme und allgemeiner Multigramme können als Zeichen aufgefaßt werden, wobei allerdings der Umfang des Zeichenvorrats sehr ansteigt.

Für Bigramme ist $\kappa_R^{**} = \frac{1}{N^2} = 14.8\%\%$, für Trigramme $\kappa_R^{***} = \frac{1}{N^3} = 0.569\%\%$. Es kommt nur darauf an, wie sich κ_S^{**} von κ_R^{**} abhebt, und es zeigt sich, daß der runde Faktor 2 , der bei der Einzelzeichenbetrachtung auftrat, bei Bigrammen (Abb. 121) durch einen Faktor 4.5 bis 7.5 ersetzt wird: Für das

Englische liegt κ_e^{**} nach *Kullback* bei 69%% , für das Deutsche liegt κ_d^{**} nach *Kullback* und *Bauer* bei 112%% . Die Niveaus sind also deutlicher getrennt. Andererseits wird schon beim Übergang zu Trigrammen (Faktor 40 !) die Schwankung auch bei 3 000 Zeichen recht beträchtlich (Abb. 122). Es ist also dafür gesorgt, daß die Bäume nicht in den Himmel wachsen.

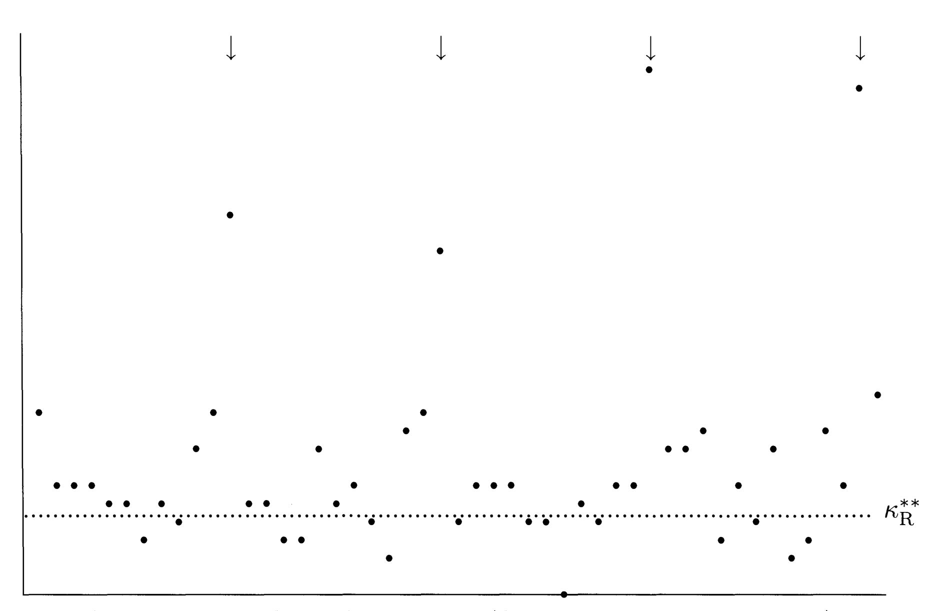


Abb. 121. Koinzidenzen für Bigramme (deutscher Text von 3 000 Zeichen)

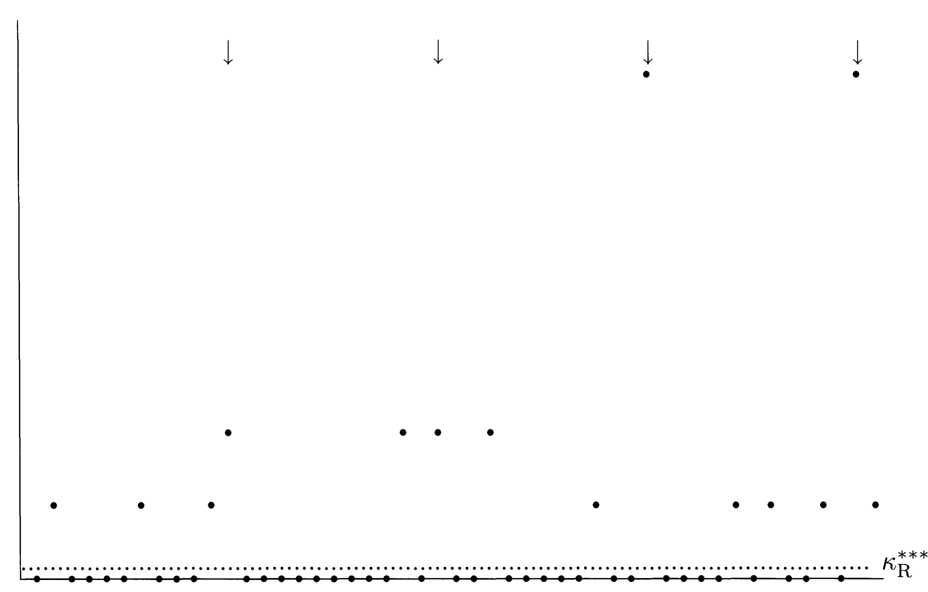


Abb. 122. Koinzidenzen für Trigramme (deutscher Text von 3 000 Zeichen)

17.3 Maschinelle Kryptanalyse

17.3.1 Daß in den U.S.A. während des 2. Weltkrieges die Methoden von *Friedman* und *Kullback* maschinell durchgeführt wurden, konnte man getrost annehmen. Schon 1932 hatte *Thomas H. Dyer* von der U.S. Navy Lochkartengeräte von I.B.M. zur Beschleunigung der Arbeit eingesetzt, die U.S. Army folgte 1936. 1941, im Jahr von Pearl Harbor, arbeiteten beim SIS (Signal Intelligence Service der U.S. Army) 13, 1945 407 Lochkarten-(Tabellier-)maschinen. I.B.M. erhielt dafür 750 000 $ Miete im Jahr.

In Deutschland wurden ebenfalls Tabelliermaschinen verwendet. Sie waren, wie auch anderswo, besonders nützlich (s. auch 18.6.3) beim ‚Abstreifen' der Überchiffrierung von Codes (9.2). Aber sie halfen auch bei der Periodenanalyse durch Kappa-Test. Zu diesem Zweck benutzten sie (nach *Kahn* und *Takagi*) auch die Japaner.

Vorläufer solcher maschineller Bearbeitung mittels Lochkartengeräten waren die Lochblätter aus Papier (*overlay sheets, perforated sheets*), die in England und anderswo verwendet wurden. Auf ihnen wurde der Geheimtext in einem binären 1-aus-26-Code durch Lochung festgehalten. Während es bei einer einmaligen Koinzidenzuntersuchung zweier Texte durchaus genügt, die beiden Texte wie in 16.1 untereinander zu schreiben, ist zur Periodenanalyse eine wiederholte Koinzidenzuntersuchung für versetzte Texte erforderlich. Dabei lohnt sich der Aufwand zur Herstellung der Lochblätter, denn Koinzidenzen verraten sich „auf einen Blick" dadurch, daß man durch die Löcher die Farbe des Tisches sieht. Diese Feststellung ist also nicht nur sicherer, sondern auch schneller. Abb. 123a zeigt ein Exemplar solcher Lochblätter, wie sie in *Bletchley Park* verwendet wurden; sie hießen dort "Banbury sheets", weil die Lochung in Banbury, einer nahegelegenen Kleinstadt erfolgte. Einzelzeichen- und auch Multigramm-Koinzidenzen sind so erkennbar (Abb. 123b).

Die Herstellung der einfachen Lochblätter kann, wie in Banbury, von Hand erfolgen. Selbstverständlich kann auch Papier gespart werden durch Verwendung geeigneter anderer Codierung, etwa in einem binären 2-aus-5-Code zur Behandlung von dezimalen Zifferncodes, oder in einem binären 2-aus-10-Code, der ausreichte, Alphabetzeichen und Dezimalziffern nebeneinander zu verarbeiten (*Willi Jensen* im OKW). Diese Codierungen, insbesondere auch die Fernschreibcodierung, erfordern jedoch kompliziertere Mechanismen zur Koinzidenzprüfung.

17.3.2 In der Chiffrierabteilung des OKW, im Jargon *Chi* genannt, wurde in der Gruppe IV „Analytische Kryptanalyse", die *Erich Hüttenhain* leitete, von *Willi Jensen* ein Spezialgerät zur Feststellung von Koinzidenzen (‚Doppler') und ihrer Abstände entwickelt. Das ‚Perioden- und Phasensuchgerät' arbeitete mit zwei identischen 5-Kanal-Fernschreiber-Lochstreifen, die zur Schleife geklebt waren, wobei in der einen Schleife eine zusätzliche Leerlochung war. Bei jedem Umlauf durch zwei Abtaster verschoben sich so die Phasenlagen der Streifen gegeneinander um *eine* Stelle (‚Sägebock-Prinzip'). Die photo-

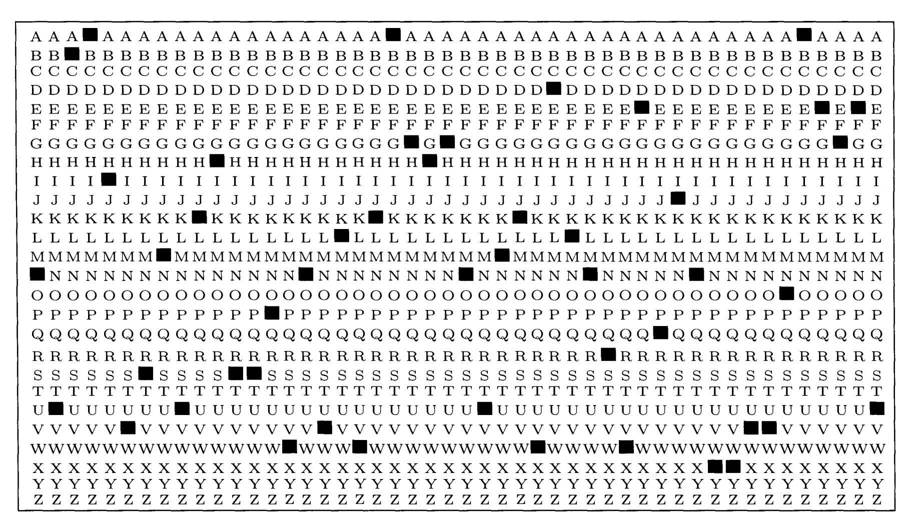


Abb. 123a. Lochblatt (*overlay sheet*) mit Ausschnitt aus dem Geheimtext von *G. W. Kulp*
NUBAIVSMUKHSSPWNVLWKAGHGNUMKWDLNRWEQJNXXVVOAEGEU

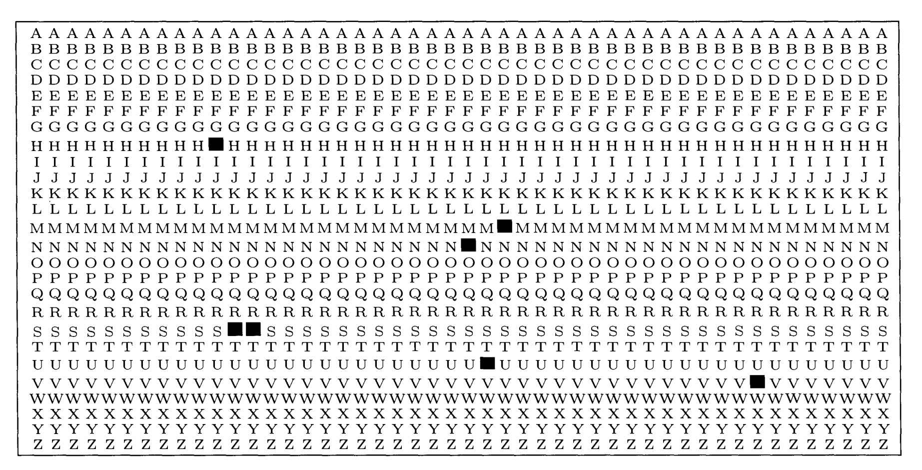


Abb. 123b. Überlagerung zweier Lochblätter mit um 72 Zeichen versetzten Ausschnitten aus dem Geheimtext von *G. W. Kulp*:

NUBA I V SMUKHSSPWNVLWKAGH GNUMKWDL N R WEQJNXXV V OAEG E U
CFPXHWZK EXHSSF X K I Y A HULMKNUMY E XDMW B X Z SBCHVW Z XPHWL
*** *** *

elektrischen Abtaster arbeiteten auf einem ‚Zeichenvergleichslabyrinth' aus Relais, das auf Zeichengleichheit prüfte und im bejahenden Fall eines Dopplers auf einem Schreibwerk einen Strich machte. Traten für eine gegebene Phasenlage mehrere Doppler auf, so wurden ebensoviele Striche aneinandergehängt. Nach einem vollständigen Umlauf rückte das Schreibwerk um eine Stelle vor. Ein zweites Schreibwerk zählte die Anzahl zweier unmittelbar aufeinanderfolgender Doppler, die Doppel-Bigramme, ein drittes die Anzahl dreier solcher, die Doppel-Trigramme usw. bis hinauf zu Parallelstellen der

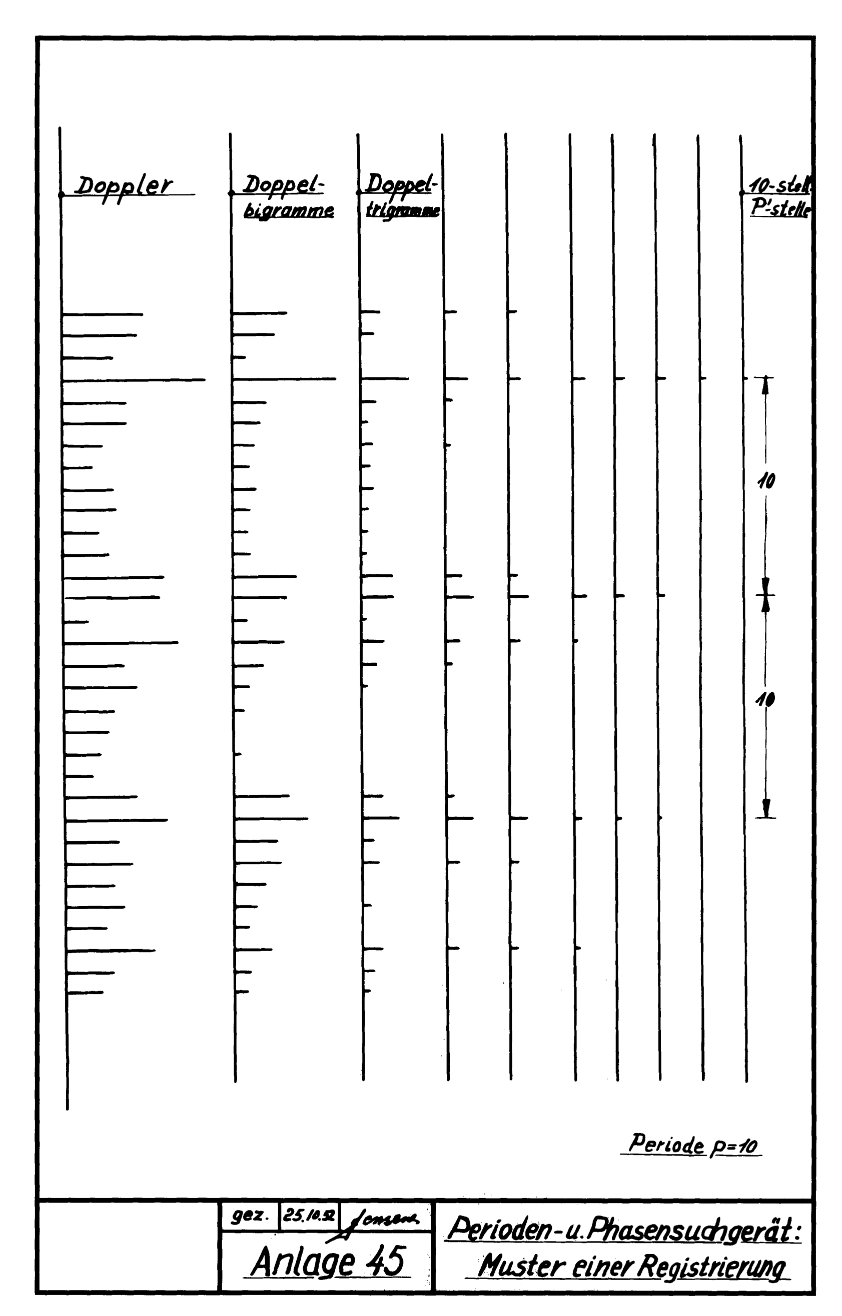


Abb. 124. Registrierung mittels des Perioden- und Phasensuchgeräts
Aus: *Willi Jensen*, Hilfsgeräte der Kryptographie. Dissertationsentwurf 1953

Länge 10 (Abb. 124). Das Gerät gab automatisch eine vollständige Friedman-Untersuchung. Bei einer Abtastgeschwindigkeit von 50 Zeichen pro Sekunde geschah dies für einen Text von 600 Zeichen in 2 Stunden, hundertmal schnel-

ler als von Hand. Das Gerät wurde bei Kriegsende zerstört. Die verfügbaren Unterlagen über *Chi* enthalten keinen Hinweis auf *Friedman*, doch darf angenommen werden, daß zumindest dessen frühe, noch veröffentlichte Arbeiten *Hüttenhain* bekannt waren. Sein Hauptwerk von 1938–1941[1] war nicht öffentlich zugänglich.

17.3.3 In Großbritannien wurde zur Mechanisierung des manuellen Arbeitens mit Lochblättern das Gerät HEATH ROBINSON[2] gebaut. Die von *C. E. Wynn-Williams* entworfene Maschine (erstes Exemplar fertig Mai 1943) hatte Vergleicher- und Zählschaltungen und konnte photoelektrisch zwei Fernschreiber-Lochstreifen mit bis zu 2 000 Zeichen pro Sekunde ablesen. Nach *Donald Michie* war die Arbeitsweise des HEATH ROBINSON vergleichbar dem ‚Sägebock-Prinzip', es wäre also gut zur Koinzidenzanalyse und Parallelstellensuche (wie auch zum Aufstellen von Differenzentabellen, s. 19.3) zu gebrauchen gewesen. Tatsächlich diente es, sobald *W.M. Tutte* die innere Struktur des Chiffrier-Fernschreibers SZ42 aufgeklärt hatte (19.2.6), hauptsächlich zur fortwährend verschobenen $\mathbb{Z}_2$-Addition eines Schlüsselstreifens zum Geheimtext, die zur Bestimmung der richtigen Phasenlage diente.

SUPER ROBINSON konnte mit vier Lochstreifen arbeiten, man nannte die Maschine auch DRAGON (von 'dragging text through'). Während man in Bletchley Park elektronisch arbeitete, war die U.S. DRAGON mit Relais aufgebaut.

Weitere Verbesserungen nahmen die Briten dann bei den COLOSSUS genannten Auswertungsmaschinen vor, die jedoch wesentlich komplexere, speziell auf Chiffrier-Fernschreiber (vgl. 9.1.3, 9.1.4) gerichtete Operationen elektronisch durchführen ließen. Mehr darüber in 18.6.3 und 19.2.6 .

Im COLOSSUS (erstes Exemplar fertig Dezember 1943, im Einsatz Februar 1944) war nur noch *ein* Lochstreifen – mit 5 000 Zeichen pro Sekunde – photoelektrisch abzulesen; die Rolle des zweiten, kürzeren und ständig zyklisch umlaufenden wurde nach *Good* von internen Röhrenschaltungen (mit etwa 1500 Röhren) übernommen. Es ist aber nicht klar, ob das Gerät in *Bletchley Park* auch zur Periodenanalyse, zum Ausrichten der Phase, zum Abstreifen einer Überchiffrierung oder auch anderswie eingesetzt wurde.

17.3.4 Über amerikanische Spezialgeräte zur Periodenanalyse durch Kappa-Test ('IC') ist neuerdings durch das Buch von *C. Burke* mehr bekannt. Schon

---

[1] *William F. Friedman*, Military Cryptanalysis, War Department, Office of the Chief Signal Officer. Washington, D.C.: U.S. Government Printing Office. Vol. I: Monoalphabetic Substitution Systems 1938, 1942[3]. Vol. II: Simpler Varieties of Polyalphabetic Substitution Systems 1938, 1943[3]. Vol. III: Simpler Varieties of Aperiodic Substitution Systems 1938, 1939[2]. Vol. IV: Transposition and Fractionating Systems 1941. Eine Kopie befindet sich in der University of Pennsylvania Library, Philadelphia, PA.

[2] *W. Heath Robinson* war ein britischer Karikaturist, der prachtvolle unpraktische Maschinen für alle möglichen und unmöglichen Aufgaben zeichnete. Nachbauten wurden u.a. PETER ROBINSON und ROBINSON AND CLEAVER (Namen Londoner Kaufhäuser) genannt.

1937 begann *Vannevar Bush* (1890–1974), der durch Analogrechner für die Lösung von Differentialgleichungen ('Differential Analyser') bekannt geworden war, für OP-20-G, den Entzifferungsdienst der U.S. Navy, nach Spezifikationen seines Leiters *Joseph Wenger* ein Gerät zur Koinzidenzzählung zu bauen, das er COMPARATOR nannte. Es arbeitete ebenfalls in einem 1-aus-26-Code. Statt jedoch wie die Briten zunächst auf bewährte Technologien zurückzugreifen, hatte *Bush* hochfliegende Pläne: photoelektrische Abtastung, elektronische Zähler (im 1-aus-10-Code). 1937 war es ein Wagnis, ein Gerät mit über hundert Vakuumröhren zum Funktionieren zu bringen. Das Projekt scheiterte auch aus bürokratischen Gründen mehrmals; daß es fortgesetzt wurde, ist vielleicht mit der Rolle, die *Bush* als Direktor des *National Defense Research Committee* (später *Office of Scientific Research and Development*) während des Krieges spielte, zu erklären. Das brachte Admiral *Stanford Caldwell Hooper*, Chef der *Naval Communications*, der ein Verfechter der ohne intuitive Eingriffe ablaufenden *pure cryptanalysis* war, und seinen Gehilfen *Joseph Wenger* nicht nur um ihren unmittelbaren Erfolg, OP-20-GY fiel im Einsatz von Maschinen zurück. Spätestens 1941 waren die U.S.A. in ihren kryptanalytischen Fähigkeiten zum Einbruch in maschinenchiffrierte Verbindungen von Großbritannien überholt worden.

Pure cryptanalysis hatte jedoch unter den mathematisch eingestellten Kryptologen Anhänger. Eine kleine Gruppe, die sich die Hilfe der erfahrenen *Agnes Meyer Driscoll* zunutze machte, ging unter *Howard T. Engstrom* gegen die ENIGMA mit Methoden der *pure cryptanalysis*, wie sie sich gegen japanische Rotormaschinen bewährt hatten, vor; für sie wurde 1942–1943 HYPO ('Hypothetical Machine') gebaut. Speziell gegen die japanischen Rotormaschinen gerichtet waren dann die Relaismaschinen VIPER und PYTHON (entwickelt um 1943) und Abkömmlinge wie der elektronische RATTLER.

17.3.5 Der von *Kullback* 1935 vorgeschlagene Chi-Test wurde, weil er über reines Zählen hinaus Additionen und Multiplikationen erforderte, zunächst (1937) nicht in Betracht gezogen; er wurde 1940 aufgegriffen und kam ab 1944 in den RAM-Maschinen ("Rapid Analytical Machines") zum Zuge. Auch die COLOSSUS-Maschinen konnten prinzipiell eine Kullback-Untersuchung durchführen, aber ob und in welchem Ausmaß das geschah, ist nicht klar.

Sobald die elektronischen Universalrechner (erste Ansätze waren DEMON, OMALLEY, HECATE, WARLOCK gegen Ende der vierziger Jahre) ausgereift waren, wurden sie kryptanalytisch eingesetzt; der Weg führte zunächst zu GOLDBERG[3], einem verbesserten COMPARATOR, und dann zu den Computern ATLAS I und ATLAS II (= ERA 1101, 1103). Zu Beginn der fünfziger Jahre verlagerte sich die kryptanalytische Massenarbeit in die Programmierung von Universalrechnern mit schneller Sonderarithmetik. Am Ende dieser Entwicklung steht vorläufig die Architektur der ab 1976 entwickelten CRAY-Supercomputer (Farbtafel Q).

---

[3] nach Rube Goldberg, amerikanisches Gegenstück zu Heath Robinson.

17.4 Parallelstellensuche nach Kasiski

Als Grenzfall des Kappa-Tests für Multigramme bestimmt man *alle* echten Multigramme, die sich wiederholen, und die Abstände, in denen sie sich wiederholen. Diese ‚Parallelstellensuche' publizierte 1863 wohl als erster *F. W. Kasiski*; vor *Friedman* und *Kullback* war sie das bevorzugte systematische Angriffsmittel professioneller Entzifferer und machte dem bis dahin weitverbreiteten Glauben an die Unbrechbarkeit polyalphabetischer Chiffrierung (8.4.1) zumindest im periodischen Fall den Garaus.

17.4.1 Doch beginnen die unsystematischen Angriffe auf polyalphabetische Chiffrierungen, kaum nachdem diese erfunden sind. Schon *Porta* hatte gelegentlich Glück mit Probieren — *OMNIA VINCIT AMOR* war der (zu) kurze und keineswegs ausgefallene Schlüssel, den ein Stümper benutzte; es kostete *Porta* weniger als eine Stunde, ihn zu erraten und die Chiffrierung zu brechen. Er selbst benutzte nur lange Schlüssel und riet, belanglose Wörter zu verwenden, die fernab vom täglichen Gebrauch liegen. Und *Giovanni Batista Argenti*, dem sein damaliger Dienstherr, *Iacomo Boncampagni*, Herzog von Sora — Neffe von Papst *Gregor* XIII — das Kryptogramm

Q A E T E P E E E A C S Z M D D F I C T Z A D Q G B P L E A Q T A I U I

gab, um seine Kunstfertigkeit zu testen, löste es, wie er schrieb, am 8. Oktober 1581 in kurzer Zeit; den Schlüssel *INPRINCIPIOERATVERBUM* erratend und die Tatsache, daß der Herzog 10 involutorische Alphabete benutzt hatte von der Art, die *Porta* 1563 beschrieben hatte (7.4.4, Abb. 53) — warum hätte der Herzog sich auch etwas Neues einfallen lassen sollen? Der Klartext war der Beginn der Æneis des *Vergil*: *arma virumque cano* ... .

Porta hatte jedoch auch schon eine methodische Idee: Wenn in der Frühform polyalphabetischer Chiffrierungen das Alphabet mit jedem Schritt (im Gegensatz zur *tabula recta*, vgl. 8.1.2) um einen Platz nach *rechts* verschoben wurde, brachten häufig vorkommende Bigramme wie /ab/, /hi/, /op/ oder gar Trigramme wie /def/ (in *deficio*) oder /stu/ (in *studium*) Buchstabenwiederholungen zustande. *Porta* fand einmal MMM und im Abstand von 51 Plätzen nochmals MMM und schloß daraus, daß der Schlüssel die Periode 17 habe und dreimal wiederholt worden sei — die Periode 51 wäre damals zu lange, die Periode 3 für einen gewitzten Chiffrierer zu kurz gewesen.

Um Haaresbreite hätte bereits *Porta Kasiski*s Methode gefunden, hätte er begriffen, daß es gar nicht auf das Wiederholungsmuster *111* ankam, sondern nur auf die Wiederholung *irgend eines* Geheimtextfragments, auf das Vorkommen einer ‚Parallelstelle', hervorgerufen durch ein Zusammentreffen eines häufig auftretenden Klartextfragments mit ein und dem selben Stück eines Schlüssels, was nur im Abstand eines Vielfachen der Periode möglich ist. Hätte *Porta* das bemerkt und publiziert, wären polyalphabetische Chiffrierungen nicht noch zu Zeiten von *Edgar Allen Poe* unangreifbar gewesen.

Nachfolgendes Beispiel von *Kahn* mag dies erläutern: Angenommen, ein VIGENÈRE-Verfahren in $\mathbb{Z}_{26}$ arbeitet mit einem kurzen Schlüssel *RUN*:

t o b e o r n o t t o b e t h a t i s t h e q u e s t i o n
R U N R U N R U N R U N R U N R U N R U N R U N R U N R U N
K I O V I E E I G K I O V N U R N V J N U V K H V M G Z I A

Hier trifft das Schlüsselfragment *RUNR* im Abstand 9 das gleiche Klartextfragment /tobe/ und ergibt die Parallelstelle KIOV, überdies trifft das Schlüsselfragment *UN* im Abstand 6 das gleiche Klartextfragment /th/ und ergibt die Parallelstelle NU. Die Abstände 9 und 6 müssen Vielfache der Periode sein, die damit nur den Wert 3 (oder 1) haben kann.

Ein ähnliches Beispiel mit einem Schlüssel *COMET* der Länge 5 lautet:

t h e r e i s a n o t h e r f a m o u s p i a n o p l a y
C O M E T C O M E T C O M E T C O M E T C O M E T C O M E
V V Q V X K G M R H V V Q V Y C A A Y L R W M R H R Z M C

In diesem Beispiel sind die Abstände der Parallelstellen 10 und 15, die Periode kann damit nur den Wert 5 (oder 1) haben.

17.4.2 Zehn Jahre vor *Kasiski* ahnte vielleicht *Babbage* schon etwas. Er, der gerne die chiffrierten Botschaften in den *'agony columns'* der viktorianischen Londoner Gazetten las, machte sich auch über Polyalphabetisches mit Wortzwischenraum her, unter reichlicher Benutzung wahrscheinlicher Wörter. Bei solchen Lösungsversuchen entwickelte er, wie man aus seinen Aufzeichnungen ersehen kann, sicher großes Verständnis für die Periodizität, aber selbst wenn er die Parallelstellensuche benutzt haben sollte – publiziert hat er sie nicht.[4] So fiel das Verdienst, einen systematischen Angriff auf polyalphabetische Chiffrierungen gefunden und verbreitet und damit die moderne Kryptologie eröffnet zu haben, einem pensionierten preußischen Infanteriemajor zu, der jedoch zu seiner Zeit dafür noch nicht berühmt wurde und sich enttäuscht der Naturgeschichte zuwandte.

Friedrich W. Kasiski wurde am 29. November 1805 in Schlochau, Westpreußen geboren. Er trat 1822 ins ostpreußische 33. Füsilier-Regiment Graf Roon ein. Dort diente er bis 1852 und wurde verabschiedet mit dem Rang eines Majors. 1863 erschien bei Mittler & Sohn in Berlin, einem renommierten Verlag, sein Büchlein, 95 Seiten stark: „Die Geheimschriften und die Dechiffrirkunst". Sein Werk führte zu einer Revolution in der Kryptologie, aber die setzte erst nach *Kasiski*s Tod am 22. Mai 1881 ein. *Kerckhoffs* würdigt *Kasiski* in einer wichtigen Arbeit von 1883, die Bücher von *de Viaris* 1893 und *Delastelle* 1902 bauen darauf auf. Um die Jahrhundertwende ist die Revolution vollzogen, ist die Angreifbarkeit periodischer polyalphabetischer Chiffrierungen unter Fachleuten allgemein bekannt.

---

[4] *Babbage* ist zwar ein Vorläufer von *de Viaris* in der Beschreibung von linearen Chiffrierungen durch mathematische Gleichungen (vgl. 7.4.1, Fußnote 4) und insofern *Kasiski* weit voraus; aber ihn als Erfinder der Parallelstellensuche zu bezeichnen, wie es *Ole Immanuel Franksen* 1984 getan hat und *Beutelspacher* (2. Aufl., 1991) es ungeprüft übernommen hat, ist nicht gerechtfertigt. Wenn *Babbage* 1846 polyalphabetische Chiffren gebrochen hat, dann lineare durch Schlüsselrekonstruktion mit Hilfe eines ‚wahrscheinlichen Worts' (vgl. 14.4.1), unter Heranziehung der bei Amateuren beliebten Wortfuge.

Im Licht von *W. F. Friedmans* Entdeckung von 1925 des *index of coincidence* erscheint die *Kasiski*sche Parallelstellenanalyse als ein rohes Verfahren. Bigramm-Parallellen werden, weil sie häufig sind, meist gar nicht beachtet, und Einzelzeichen-Parallelen ohnehin nicht – hingegen mißt das *Kappa* alle Parallelen und fragt nur, ob es überdurchschnittlich viele sind. Daß man Bigramm-Parallelen i.a. nicht beachtet, rührt davon her, daß sie auch „zufällig" zustande kommen können. Selbst bei Trigrammen passiert das noch häufig, es kann aber auch bei höheren Multigrammen vorkommen und stört die Analyse – beim *index of coincidence* kümmert das gar nicht. Die *Kasiski*sche Methode nimmt jedoch als Periode den größten gemeinsamen Teiler der Parallelen-Abstände unter pragmatischer Ausschließung einiger als störend angesehenen „zufälligen" Parallelen. In dieser Hinsicht ist sie sehr intuitiv und nicht mechanisierbar. Überdies erfordert die Kasiski-Untersuchung auch etwas längere Texte, um überhaupt fündig zu werden.

„Zufällige" Parallelen treten gerade bei linearen Substitutionen häufiger auf. Grund dafür ist das Kommutativgesetz, das für die Summenbildung *modulo N* gilt: /anton/ mit dem Schlüssel *BERTA* liefert das gleiche wie /berta/ mit dem Schlüssel *ANTON*. Dieser Effekt tritt also besonders auf, wenn der Schlüsseltext aus dem selben Genre ist wie der Klartext. Auch Parallelstellen im Schlüsseltext können zu „falschen" Geheimtext-Parallelstellen führen – Schlüssel wie *DANSEUSECANCAN*, *VIERUNDVIERZIG* können den unbefugten Entzifferer zum Narren halten.[5]

17.4.3 Die Schulbeispiele für *Kasiski*s Methode in der Literatur sind fast immer aufgemacht und zeigen mehr Parallelstellen, als man im Mittel erwarten darf. Von folgendem Beispiel (*Kahn*) kann man das nicht sagen. Der Klartext ist, wie sich später zeigen wird, ein beherzigenswerter Ratschlag von *Albert J. Myer*, U.S. Signal Corps (1866). Der Geheimtext lautet

```
ANYVG YSTYN RPLWH RDTKX RNYPV QTGHP
HZKFE YUMUS AYWVK ZYEZM EZUDL JKTUL
JLKQB JUQVU ECKBN RCTHP KESXM AZOEN
SXGOL PGNLE EBMMT GCSSV MRSEZ MXHLP
KJEJH TUPZU EDWKN NNRWA GEEXS LKZUD
LJKFI XHTKP IAZMX FACWC TQIDU WBRRL
TTKVN AJWVB REAWT NSEZM OECSS VMRSL
JMLEE BMMTG AYVIY GHPEM YFARW AOAEL
UPIUA YYMGE EMJQK SFCGU GYBPJ BPZYP
JASNN FSTUS STYVG YS
```

[5] Auf diese Symmetrie werden wir in 18.5 noch zu sprechen kommen.

Die Häufigkeitsverteilung zeigt Abb. 125; sie ist viel zu gleichmäßig, um die einer monoalphabetischen Substitution oder einer Transposition zu sein. Also ist an eine polyalphabetische Substitution zu denken. Darauf deutet auch das reichliche Vorkommen von Parallelstellen hin. Es finden sich neun Parallelstellen der Länge 3 und mehr, darunter sehr lange wie LEEBMMTG und CSSVMRS. Ihre Abstände sind in Abb. 126 aufgelistet.

14	8	7	5	22	6	12	8	5	11	14	13	16	13	4	13	5	11	18	15	14	10	9	7	16	11
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Abb. 125. Häufigkeitsverteilung im Geheimtext von *Kahn*

Fragment	Abstand	Primfaktorzerlegung
YVGYS	280	$2^3 \cdot 5 \cdot 7$
STY	274	$2 \cdot 137$
GHP	198	$2 \cdot 3^2 \cdot 11$
ZUDLJK	96	$2^5 \cdot 3$
LEEBMMTG	114	$2 \cdot 3 \cdot 19$
CSSVMRS	96	$2^5 \cdot 3$
SEZM	84	$2^2 \cdot 3 \cdot 7$
ZMX	48	$2^4 \cdot 3$
GEE	108	$2^2 \cdot 3^3$

Abb. 126. Faktorzerlegung von Parallelstellen-Abständen

Folgt man *Kasiski* wörtlich, so muß man „die Abstände in Faktoren zerlegen, der am häufigsten gefundene Faktor gibt die Periode an". Die Literatur deutet das, *M. E. Ohaver* folgend, gelegentlich dahingehend, daß alle Faktoren aufzuschreiben sind (Abb. 127). Dabei könnte es vorkommen, daß es zwei häufigste Faktoren gibt und man eine willkürliche Entscheidung treffen muß. Die richtige Regel lautet, daß man den größten gemeinsamen Teiler der Abstände aller „echten" Parallelen nehmen muß – aber welche echt sind, weiß man noch nicht. Gerne ließe man „störende" Parallelstellen weg, also solche, deren Abstand einen sonst vorherrschenden Faktor nicht enthält – in Abb. 126 wären das STY sowie YVGYS, wobei man nicht geneigt ist, von letzterem wegen seiner Länge 5 anzunehmen, daß es zufällig entstanden ist. Läßt man es jedoch nicht weg, so wäre 2 die Periode, was auch kaum zutreffen kann. Die Periode 12 hätte man, wenn man auch noch annehmen würde, daß GHP sowie LEEBMMTG zufällig entstanden wären. Bei ersterem kann man sich das vorstellen, bei letzterem kaum. Also muß man mit der Vermutung, daß 6 die Periode ist, leben.

Zweifellos zeigt dies eine schwache Seite der Kasiski-Untersuchung. Um so wichtiger ist, daß die Friedman-Untersuchung und die noch zu besprechende Kullback-Untersuchung zuverlässiger sind. Ein durch eine zufällige Parallelstelle hervorgerufener zu kleiner Wert für die angebliche Periode stört die gesamte Methode. Andererseits kann es vorkommen, daß der größte gemeinsame Teiler aller Parallelstellenabstände ein Vielfaches der Periode ist. In diesem Fall tritt nur eine unnötige Vermehrung des Arbeitsaufwands ein und eine Erschwerung der darauf folgenden Aufstellung der einzelnen Alphabete.

Fragment	Abstand	2	3	4	5	6	7	8	9	10	11	12	14	16	18	19	20	21	22	24	
YVGYS	280	√		√	√		√	√		√			√				√				(unecht?)
STY	274	√																			(unecht?)
GHP	198	√	√			√			√		√				√				√		
ZUDLJK	96	√	√	√		√		√				√		√						√	
LEEBMMTG	114	√	√			√											√				
CSSVMRS	96	√	√	√		√		√				√		√						√	
SEZM	84	√	√	√		√	√					√	√					√			
ZMX	48	√	√	√		√		√				√									
GEE	108	√	√	√		√			√			√			√						

Abb. 127. Faktoren der Parallelstellen-Abstände

Der späteren Entzifferung (18.1) vorgreifend, merken wir schon an, daß sich STY und YVGYS als unechte Parallelstellen herausstellen werden, und zwar kommen sie aufgrund der Kommutativität einer linearen Substitution über $\mathbb{Z}_{26}$ zustande: Der Schlüssel ist *SIGNAL*, und YVGYS entsteht das erste Mal aus /signa/+*GNALS*, das zweite Mal aus /gnals/+*SIGNA*; STY entsteht das erste Mal aus /als/+*SIG*, das zweite Mal aus /sig/+*ALS*. Man erkennt, daß dieser Effekt durch die Verwendung des Schlüsselworts *SIGNAL* aus dem Genre des Klartextes hervorgerufen wurde. Er bringt für den unbefugten Entzifferer eine Erschwerung und ist deshalb für den Kryptographen erwünscht. Er tritt im übrigen auch bei den Kappa- und Chi-Tests verfälschend in Erscheinung.

Zufällige Parallelstellen können aber auch anders zustande kommen. Der große französische Kryptologe *Étienne Bazeries* hatte einmal Pech mit einer BEAUFORT-Chiffrierung: In einer Depesche von 1898 des aufrührerischen Herzogs von Orléans (*Bazeries*' I in der fünften Gruppe müßte ein J sein)

GNJLN RBEOR PFCLS OKYNX TNDBI LJNZE OIGSS HBFZN ETNDB JJMZQ .....

fand er eine Parallelstelle TNDB der Länge 4 im Abstand 21. Eine kürzere Parallelstelle EO der Länge 2 trat im Abstand 22 auf – sie stellte sich schließlich als echt heraus. *Bazeries* aber hatte natürlich zu der längeren Parallelstelle größeres Vertrauen. Die weitere Untersuchung mit der angeblichen Periode 21 führte ihn zunächst in die Irre und hielt ihn lange auf. Die Parallelstelle TNDB war zufällig entstanden durch *ERVE* −/lesd/ bzw. durch *IERV* −/prou/ (Schlüssel: *VENDREDIDIXSEPTFEVRIER*). *Bazeries* bemerkte bitter: ≪*En cryptographie, aucune règle n'est absolu.*≫

17.4.4 Die Kasiski-Untersuchung wurde trotz ihrer offensichtlichen Schwächen auch im 2. Weltkrieg noch häufig angewendet. In der Chiffrierabteilung des OKW (im Jargon *Chi*) wurde (neben dem ‚Perioden- und Phasensuchgerät', 17.3.2) ein spezielles Parallelstellensuchgerät entwickelt (*Willi Jensen*) und praktisch eingesetzt. Der Geheimtext wurde auf Filmstreifen gestanzt in doppelter Ausfertigung in einem 2-aus-10-Code, der auch eine Mischung von Buchstaben (Z_{26}) und Ziffern (Z_{10}) zu verarbeiten gestattete. Eine Kopie (A) wurde zum Ring geklebt und lief dauernd an einem Abtaster vorbei, während

der zweite Filmstreifen (B) bei jedem Umlauf des ersten um *ein* Zeichen in seinem Abtaster vorrückte. Bei Übereinstimmung zweier Zeichen decken sich zwei Löcher, andernfalls eines oder keines. Eine Photozelle ist in der Lage, den Lichtmengenunterschied zu messen; durch eine Blende veränderlicher Breite ist es möglich, in jeweils einem Gang auch Bigramm-, Trigramm-, Tetragramm- usw. Parallelen festzustellen; innerhalb der verfügbaren Meßgenauigkeit konnten bis zu zehnstellige Parallelstellen gesucht werden. Die Registrierung der Lage einer gefundenen Parallelstelle erfolgte automatisch durch Funkenüberschlag auf einer Aluminiumfolie; die zweidimensionale Aufzeichnung gibt die Lage auf (A) sowie auf (B) wieder. Das Gerät war auf schnelle Bearbeitung großer Mengen von Texten hin entwickelt; durch den Abtaster sollten 10^4 Zeichen pro Sekunde geschickt werden – in knapp drei Stunden war ein Textkonvolut von 10 000 Zeichen, das 10^8 Vergleiche erforderte, behandelt. Das Gerät wurde bei Kriegsende zerstört, bevor es länger praktisch erprobt werden konnte. In den U.S.A. baute *Vannevar Bush* 1943 für OP-20-G ein ähnliches Gerät, TETRA (Spitznamen ICKI, TESSIE, siehe 18.6.3), das ebenfalls Parallelstellen mit weiten Abständen finden sollte. Mitte 1944 begann man unter Friedman, eine mit Mikrofilm arbeitende universelle kryptanalytische Maschine mit der Bezeichnung 5202 zu entwickeln.

17.4.5 Photoelektrische Abtastung, die auf deutscher, britischer und amerikanischer Seite herangezogen wurde, geht auf Maschinen zur Dokumentsuche zurück, für die in Berlin *Michael Maul* 1927 und *Emanuel Goldberg* 1928 Patente bekamen. *Vannevar Bush*'s Pläne für den COMPARATOR liefen parallel zur Entwicklung des RAPID SELECTOR, der zu einem Dokumentationssystem ('Memex') führen sollte.

17.5 Kolonnenbildung und Phi-Test nach Kullback

Ein einfaches mechanisches Mittel zur Feststellung von Koinzidenzen besteht darin, den Geheimtext nach einer vermuteten Periode d in Kolonnen T_1, T_2, T_3, …, T_d anzuordnen (**Kolonnenbildung**, engl. '*writing out a depth*').

Abb. 128 zeigt das Ergebnis für den Geheimtext von *G. W. Kulp* mit $d = 12$. Die Doppler mit dem Minimalabstand d stehen unmittelbar untereinander und fallen sofort auf, etwa z ganz rechts in der ersten und der zweiten Zeile. Aber auch Doppler im Abstand von $k \cdot d$ findet man leicht, etwa ein weiteres z ganz rechts in der drittletzten Zeile. Auch Doppler-Bigramme zeigen sich, die in verschiedenen Zeilen an gleicher Stelle stehen, etwa das Bigramm WK in der vierten und siebten Zeile, das Bigramm MW in der zweiten und elften Zeile, das Bigramm WZ in der zwölften und vorletzten Zeile, schließlich das Bigramm NU, das in der sechsten, achten und drittletzten Zeile zu finden ist.

17.5.1 Macht man sich aber schon die (geringe) Mühe, den Geheimtext in Kolonnen umzuordnen, so kann man sofort mehr herausholen. Jede Kolonne T_ρ ist ja mit dem selben Alphabet chiffriert, wenn die Periode getroffen wurde; andernfalls aber mit verschiedenen Alphabeten. Bildet man also

	G	E	I	E	I	A	S	G	D	X	V	Z	
	I	J	Q	L	M	W	L	A	A	M	X	Z	
	Y	Z	M	L	W	H	F	Z	E	K	E	J	
	L	V	D	X	W	K	W	K	E	T	X	L	
	B	R	A	T	Q	H	L	B	M	X	A	A	
	N	U	B	A	I	V	S	M	U	K	H	S	
	S	P	W	N	V	L	W	K	A	G	H	G	
	N	U	M	K	W	D	L	N	R	W	E	Q	
	J	N	X	X	V	V	O	A	E	G	E	U	
	W	B	Z	W	M	Q	Y	M	O	M	L	W	
	X	N	B	X	M	W	A	L	P	N	F	D	
	C	F	P	X	H	W	Z	K	E	X	H	S	
	S	F	X	K	I	Y	A	H	U	L	M	K	
	N	U	M	Y	E	X	D	M	W	B	X	Z	
	S	B	C	H	V	W	Z	X	P	H	W	L	
	G	N	A	M	I	U	K						
ϕ_r	14	16	12	16	30	16	14	14	18	12	18	10	=190

Abb. 128. Geheimtext, in Kolonnen nach der vermuteten Periode 12

$Phi(T_\rho)$ für $\rho = 1, 2, \ldots, u-1, u$, so sollte man für alle $Phi(T_\rho)$ im ersten Fall ($u = k \cdot d$) Werte nahe κ_{S} erwarten, im zweiten Fall aber nahe $\kappa_{\mathrm{R}} = \frac{1}{N}$.

17.5.2 Tatsächlich ist es am besten, über die $Phi(T_\rho)$, $\rho = 1, 2, \ldots, u{-}1, u$ zu mitteln. Mit (vgl. 16.4.1) $\phi_\rho = \sum_{i=1}^{N} m_i^\rho \cdot (m_i^\rho - 1)$, wo m_i^ρ die Häufigkeit des i-ten Zeichens in der ρ-ten Kolonne ist, bildet man also

$$Phi^{(u)}(T) = u \cdot \sum_{\rho=1}^{u} \phi_\rho / M \cdot (M-u) \quad .$$

Der Faktor u dient zur Normalisierung. (Durch Auffüllen ist $u|M$ erzielbar.)

Wie in 16.4.1 zeigt man das *Kappa*-*Phi*$^{(u)}$ **-Theorem**:

$$\frac{1}{M-1} \sum_{\rho=1}^{M-1} Kappa(T^{(u \cdot \rho)}, T) = Phi^{(u)}(T) \ .$$

$Phi^{(u)}(T)$ ist also der *Mittelwert* aller Kappa-Werte in Abständen eines Vielfachen von u und erweist sich damit als *sehr scharfes* Instrument.

17.5.3 Für $u = 12$ müssen zwölf Alphabete verwendet werden, auf jedes treffen 16 oder 15 Buchstaben. Für jede der 12 vermutlich monoalphabetisch chiffrierten Kolonnen in Abb. 128 läßt sich nun das ϕ_ρ und das ψ_ρ berechnen:

für die erste Spalte, die S und N dreifach, G doppelt hat,
$\phi_1 = 6+6+2 = 14$ bzw. $\psi_1 = 9+9+4+1+1+1+1+1+1+1+1 = 30$;
für die zweite Spalte, die N und U dreifach, B und F doppelt hat,
$\phi_2 = 6+6+2+2 = 16$ bzw. $\psi_2 = 9+9+4+4+1+1+1+1+1+1 = 32$;
für die dritte Spalte, die M dreifach, A, B und X doppelt hat,
$\phi_3 = 6+2+2+2 = 12$ bzw. $\psi_3 = 9+4+4+4+1+1+1+1+1+1+1 = 28$;
für die fünfte Spalte, die I vierfach, M, W und V dreifach hat,

	G	E	I	E	I	A	S	G	D	X	V	
	Z	I	J	Q	L	M	W	L	A	A	M	
	X	Z	Y	Z	M	L	W	H	F	Z	E	
	K	E	J	L	V	D	X	W	K	W	K	
	E	T	X	L	B	R	A	T	Q	H	L	
	B	M	X	A	A	N	U	B	A	I	V	
	S	M	U	K	H	S	S	P	W	N	V	
	L	W	K	A	G	H	G	N	U	M	K	
	W	D	L	N	R	W	E	Q	J	N	X	
	X	V	V	O	A	E	G	E	U	W	B	
	Z	W	M	Q	Y	M	O	M	L	W	X	
	N	B	X	M	W	A	L	P	N	F	D	
	C	F	P	X	H	W	Z	K	E	X	H	
	S	S	F	X	K	I	Y	A	H	U	L	
	M	K	N	U	M	Y	E	X	D	M	W	
	B	X	Z	S	B	C	H	V	W	Z	X	
	P	H	W	L	G	N	A	M	I	U	K	
ϕ_r	8	6	8	12	10	8	10	4	8	16	20	=110

Abb. 129. Geheimtext, in Kolonnen nach der vermuteten Periode 11

$\phi_5 = 12 + 6 + 6 + 6 = 30$ bzw. $\psi_5 = 16 + 9 + 9 + 9 + 1 + 1 + 1 = 46$;
für die sechste Spalte, die W vierfach, H und V doppelt hat,
$\phi_6 = 12+2+2 = 16$ bzw. $\psi_6 = 16+4+4+1+1+1+1+1+1+1+1 = 32$
usw. Abb. 128 zeigt, daß sich die Summe $\sum_{\rho=1}^{12} \phi_\rho$ zu 190 und damit $Phi^{(12)} = 12 \cdot 190/(187 \cdot 186) = 6.56\%$ ergibt. 12 könnte sehr wohl eine Periode sein.

Für $u = 11$ zeigt Abb. 129 das Ergebnis der Kolonnenbildung. Jetzt liest man sofort ab, welche Doppler-Zeichen es im Abstand 11 gibt, etwa W in der zweiten und dritten Zeile, oder mit einem Vielfachen von 11 als Abstand: V in der ersten, sechsten und siebten Zeile. Man findet übrigens keinen Doppler-Bigramme mehr.

Bildet man aber mit den 11 Alphabeten (der Länge 17) $\sum_{\rho=1}^{11} \phi_\rho$, so findet man (Abb. 129) den Wert 110 und $Phi^{(11)} = 11 \cdot 110/(187 \cdot 186) = 3.48\%$.

$Phi^{(11)}$ ist deutlich niedriger als $Phi^{(12)}$. Die Hypothese, es handle sich bei dieser Kolonnenbildung zu je elf jeweils um eine monoalphabetische Chiffrierung, wird also nicht gestützt.

Für $u = 13$ zeigt schließlich Abb. 130 das Ergebnis der Kolonnenbildung und der Bestimmung von $Phi^{(13)} = 13 \cdot 126/(187 \cdot 186) = 4.71\%$.

Nunmehr kann man den Werteverlauf von $Phi^{(u)}$ für $u = 2, 3, 4, \ldots$ betrachten (Abb. 131). Der Wert für $u = 12$ hebt sich gegenüber Abb. 116 auf diese Weise viel deutlicher heraus, so daß die vermutete Periode Zwölf durch die Kullback-Untersuchung für die weitere Arbeit gesichert erscheint. Dies be-

	G	E	I	E	I	A	S	G	D	X	V	Z	I	
	J	Q	L	M	W	L	A	A	M	X	Z	Y	Z	
	M	L	W	H	F	Z	E	K	E	J	L	V	D	
	X	W	K	W	K	E	T	X	L	B	R	A	T	
	Q	H	L	B	M	X	A	A	N	U	B	A	I	
	V	S	M	U	K	H	S	S	P	W	N	V	L	
	W	K	A	G	H	G	N	U	M	K	W	D	L	
	N	R	W	E	Q	J	N	X	X	V	V	O	A	
	E	G	E	U	W	B	Z	W	M	Q	Y	M	O	
	M	L	W	X	N	B	X	M	W	A	L	P	N	
	F	D	C	F	P	X	H	W	Z	K	E	X	H	
	S	S	F	X	K	I	Y	A	H	U	L	M	K	
	N	U	M	Y	E	X	D	M	W	B	X	Z	S	
	B	C	H	V	W	Z	X	P	H	W	L	G	N	
	A	M	I	U	K									
ϕ_r	4	4	12	10	18	10	8	12	10	10	14	8	6	=126

Abb. 130. Geheimtext, in Kolonnen nach der vermuteten Periode 13

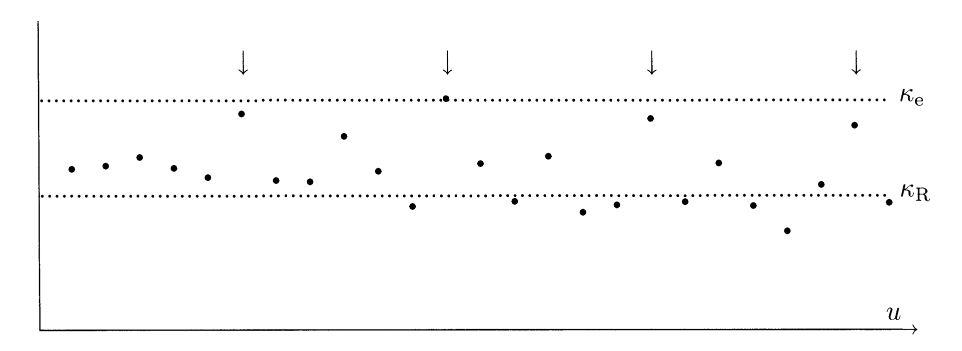


Abb. 131. *Phi*$^{(u)}$-Verlauf für den Geheimtext von *G. W. Kulp*

deutet, verglichen mit der Friedman-Untersuchung, eine Verfeinerung der Periodenanalyse durch die Kullback-Untersuchung. Aber auch für $u = 6$, 18, 24 tritt ein Effekt auf, die Periode Sechs kann nicht ausgeschlossen werden.

17.6 Eine Abschätzung für die Periodenlänge

Aus dem *Kappa-Phi*-Theorem von 16.4.1 ergibt sich für die Erwartungswerte

$$\langle Phi(T)\rangle_Q^{(M)} = \tfrac{1}{M-1}\sum_{\rho=1}^{M-1}\langle Kappa(T,T^{\rho})\rangle_Q \ .$$

Zu Beginn dieses Kapitels wurde darauf hingewiesen, daß

$$\langle Kappa(T,T^{k\cdot d})\rangle_Q = \kappa_S \ ,$$

und des weiteren, daß, wenn u kein Vielfaches von d ist, „in der Regel“

$$\langle Kappa(T,T^{u})\rangle_Q \approx \kappa_R = \tfrac{1}{N} \quad .$$

Wird der Einfachheit halber angenommen, M sei ein Vielfaches der Periode d, so ergibt sich in der Summe $\frac{M}{d}-1$ mal κ_S, die übrigen Male κ_R; also ist $\langle Phi(T)\rangle_Q^{(M)}$ eine Mittelung aus κ_S und κ_R,

$$(M-1)\cdot\langle Phi(T)\rangle_Q^{(M)} = (\tfrac{M}{d}-1)\cdot\kappa_\mathrm{S} + ((M-1)-(\tfrac{M}{d}-1))\cdot\kappa_\mathrm{R}\ .$$

Unter der Annahme, daß das beobachtete $Phi(T)$ den Erwartungswert approximiert, gilt also (*Abraham Sinkov*, um 1935)

$$(M-1)\cdot Phi(T) \quad\approx\quad (\tfrac{M}{d}-1)\cdot\kappa_\mathrm{S} + ((M-1)-(\tfrac{M}{d}-1))\cdot\kappa_\mathrm{R}\ .$$

Diese fundamentale Beziehung zeigt, wie bei gleichbleibender Quelle mit wachsender Periode einer polyalphabetischen Chiffrierung der Wert von *Phi* sich ändert. Für große M und $d \ll M$ kann man mit

$$Phi(T) \approx \tfrac{1}{d}\cdot\kappa_\mathrm{S} + (1-\tfrac{1}{d})\cdot\kappa_\mathrm{R}$$

fast ebenso gut arbeiten.

Die Beziehung von *Sinkov* läßt sich auch nach d auflösen:

$$(\frac{M}{d}-1) \approx \frac{(M-1)\cdot(Phi(T)-\kappa_\mathrm{R})}{\kappa_S-\kappa_\mathrm{R}}\ \text{, d.h.}$$

$$d \approx \frac{\kappa_\mathrm{S}-\kappa_\mathrm{R}}{(\kappa_S - Phi(T))/M + (Phi(T)-\kappa_\mathrm{R})}\ .$$

Für große M und $d \ll M$ kann man auch die Näherung benutzen

$$d \approx \frac{\kappa_\mathrm{S}-\kappa_\mathrm{R}}{Phi(T)-\kappa_\mathrm{R}}\ .$$

Beispielsweise hat man für den Geheimtext von *G. W. Kulp* mit $M = 187$, $\kappa_S = \kappa_\text{englisch} = 6.58\%$, $\kappa_\mathrm{R} = \frac{1}{N} = 3.85\%$ nach 17.1 einen Wert von *Phi* von 4.56% , dies ergibt

$$d \approx \frac{2.73\%}{(2.02\%/187)+0.71\%} = 3.79$$

bzw. nach der Näherung

$$d \approx \frac{2.73\%}{0.71\%} = 3.85\ .$$

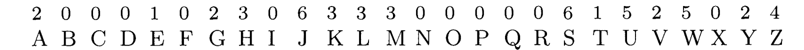
Dieser Wert ist gegenüber der vermuteten Periode $d = 12$ zu niedrig und würde besser zu $d = 6$ passen; es wäre auch nicht überraschend, wenn er zu hoch ausgefallen wäre. Zur Unterstützung einer Periodenanalyse nach *Kasiski*, *Friedman* oder *Kullback* ist die Abschätzungsformel – insbesondere bei kleinen Perioden – brauchbar; allein wäre sie wegen ihrer großen Instabilität ohne Nutzen.

18 Zurechtrücken begleitender Alphabete

Ist die Periode eines polyalphabetisch chiffrierten Geheimtexts hinlänglich zuverlässig bestimmt, so kann man nun – sofern möglich – versuchen, die einzelnen Alphabete auf ein Referenzalphabet (*primary alphabet*) zu reduzieren. Wenn es sich um VIGENÈRE-Schritte handelt, läge ein Durchprobieren aller begleitenden Standardalphabete (7.4) nahe. Genauso kann man verfahren, wenn es sich um ALBERTI-Schritte handelt *und* wenn ein Nicht-Standard-Alphabet bekanntgeworden ist. Im allgemeinen muß aber für jedes Alphabet die Verschiebung gegenüber einem unbekannten Referenzalphabet bestimmt werden. Dazu wird sich wiederum eine Kullback-Untersuchung heranziehen lassen. Der Fall unbekannter unabhängiger Alphabete, wo jedes für sich einzeln bestimmt werden muß, erlaubt dieses Vorgehen nicht.

18.1 Durchdecken der Häufigkeitsgebirge

Angesichts der weiten Verbreitung, die VIGENÈRE-Chiffrierung genießt, mag es allemal lohnend sein, den mit geringem Aufwand zu führenden Einstieg zu versuchen. Dazu sind im Fall einer Periode d gerade d Häufigkeitsgebirge zu betrachten. Mustererkennung sowie Exhaustion nach 12.5 für die einzelnen CAESAR-Additionen funktioniert nicht, da die Texte „zerrissen“ sind.



2	0	0	0	1	0	2	3	0	6	3	3	3	0	0	0	0	0	6	1	5	2	5	0	2	4
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Abb. 132. Häufigkeitsverteilung in der ersten Kolonne

18.1.1 Im Beispiel von *Myers* Text (17.4.3) bricht man am besten den Geheimtext in sechs Kolonnen und zählt für jede Kolonne die Häufigkeiten aus. Für die erste Kolonne, also für den Teiltext, der aus dem 1., dem 7., dem 13., dem 19. Zeichen usw. besteht, zeigt Abb. 132 das Ergebnis. Man erkennt sofort das Häufigkeitsgebirge des Englischen: NOPQR ist die v-w-x-y-z-Niederung, links anschließend JKLM ist der r-s-t-u-Kamm. DEFGH müßte dann, im richtigen Abstand liegend, der l-m-n-o-p-Kamm sein, was nicht

deutlich herauskommt. Aber mit solchen Schwankungserscheinungen muß der Kryptanalyst rechnen, und auch damit, daß W nicht ganz die Häufigkeit hat, die man für den e-Gipfel erwartet.

Mit *S*: S $\hat{=}$ a ist also der erste Schlüsselbuchstabe *S* eines VIGENÈRE-Schrittes gefunden: Es ist daher anzunehmen, daß es sich im ganzen um ein VIGENÈRE-System handelt und auch die anderen Chiffrierschritte auf Verschiebungen des Standardalphabets hinauslaufen. Mit ihnen verfährt man entsprechend und gewinnt Schritt für Schritt den Schlüssel

SIGNAL ;

die Bestätigung findet man durch anschließende Entzifferung. Der Klartext lautet (die zu echten Parallelstellen führenden Teiltexte sind unterstrichen)

```
i f s i g   n a l s a   r e t o b   e d i s p   l a y e d   i n t h e
p r e s e   n c e o f   a n e n e   m y t h e   y m u s t   b e g u a
r d e d b   y c i p h   e r s t h   e c i p h   e r s m u   s t b e c
a p a b l   e o f f r   e q u e n   t c h a n   g e s t h   e r u l e
s b y w h   i c h t h   e s e c h   a n g e s   a r e m a   d e m u s
t b e s i   m p l e c   i p h e r   s a r e u   n d i s c   o v e r a
b l e i n   p r o p o   r t i o n   a s t h e   i r c h a   n g e s a
r e f r e   q u e n t   a n d a s   t h e m e   s s a g e   s i n e a
c h c h a   n g e a r   e b r i e   f f r o m   a l b e r   t j m y e
r s m a n   u a l o f   s i g n a   l s
```

Man erkennt jetzt sogar, wie die Parallelstellen (17.4.3) zustande kamen: Die längste, LEEBMMTG, ergibt sich aus einem wiederholten Zusammentreffen von /frequent/ mit *GNALSIGN*; eine andere, ZUDLJK, aus dem wiederholten Zusammentreffen von /mustbe/ mit *NALSIG*. CSSVMRS entsteht aus /changes/ mit *ALSIGNA*. Andrerseits führte das wiederholte Vorkommen von /cipher/ im Klartext zu keiner Parallelstelle. SEZM, GHP, ZMX, GEE stammen daher, daß /sthe/, /the/, /her/, /are/ auf *ALSI*, *NAL*, *SIG*, *GNA* treffen. YVGYS und STY erweisen sich in der Tat als unechte Parallelen.

18.1.2 Bei relativ langen Schlüsseln mag es schwer sein, aus der Auszählung etwas zu erkennen. Am besten und auch am einfachsten ist dann eine graphische Darstellung. Für den Fall des Geheimtextes von *G. W. Kulp* (Abb. 115) sind die Vorarbeiten in Form der Kolonnenbildung für $d = 12$ in 17.5 bereits getroffen, die Arbeit kann sich unmittelbar an die Periodenbestimmung durch die Kullback-Untersuchung anschließen. Aus Abb. 128 gewinnt man unmittelbar die zwölf Häufigkeitsgebirge, die in Abb. 133 übereinanderstehen. Der Versuch hat sich auch hier gelohnt; Abb. 134 zeigt, wie man sie durch geeig-

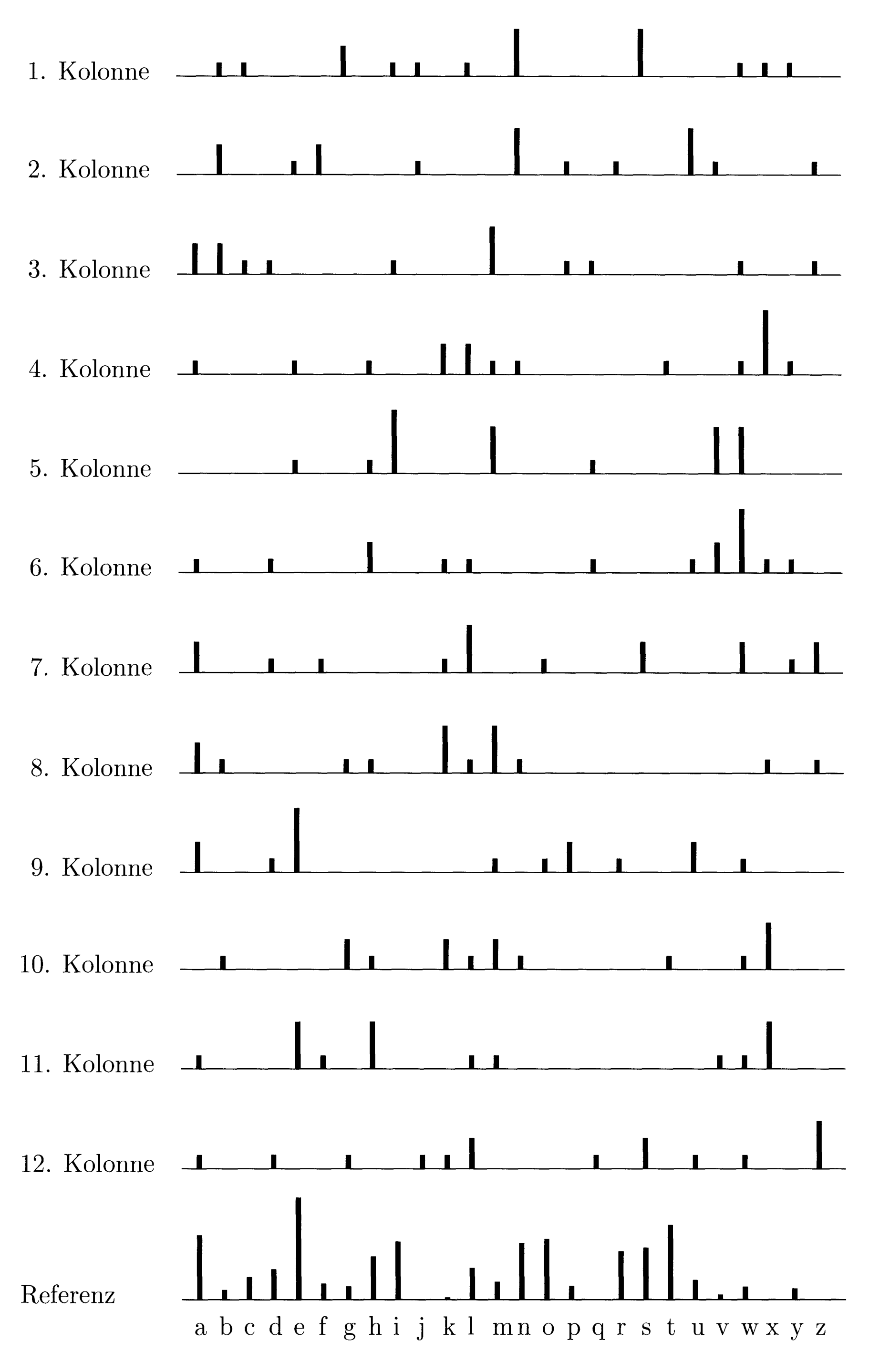


Abb. 133. Häufigkeitsgebirge für den Geheimtext von *G. W. Kulp*

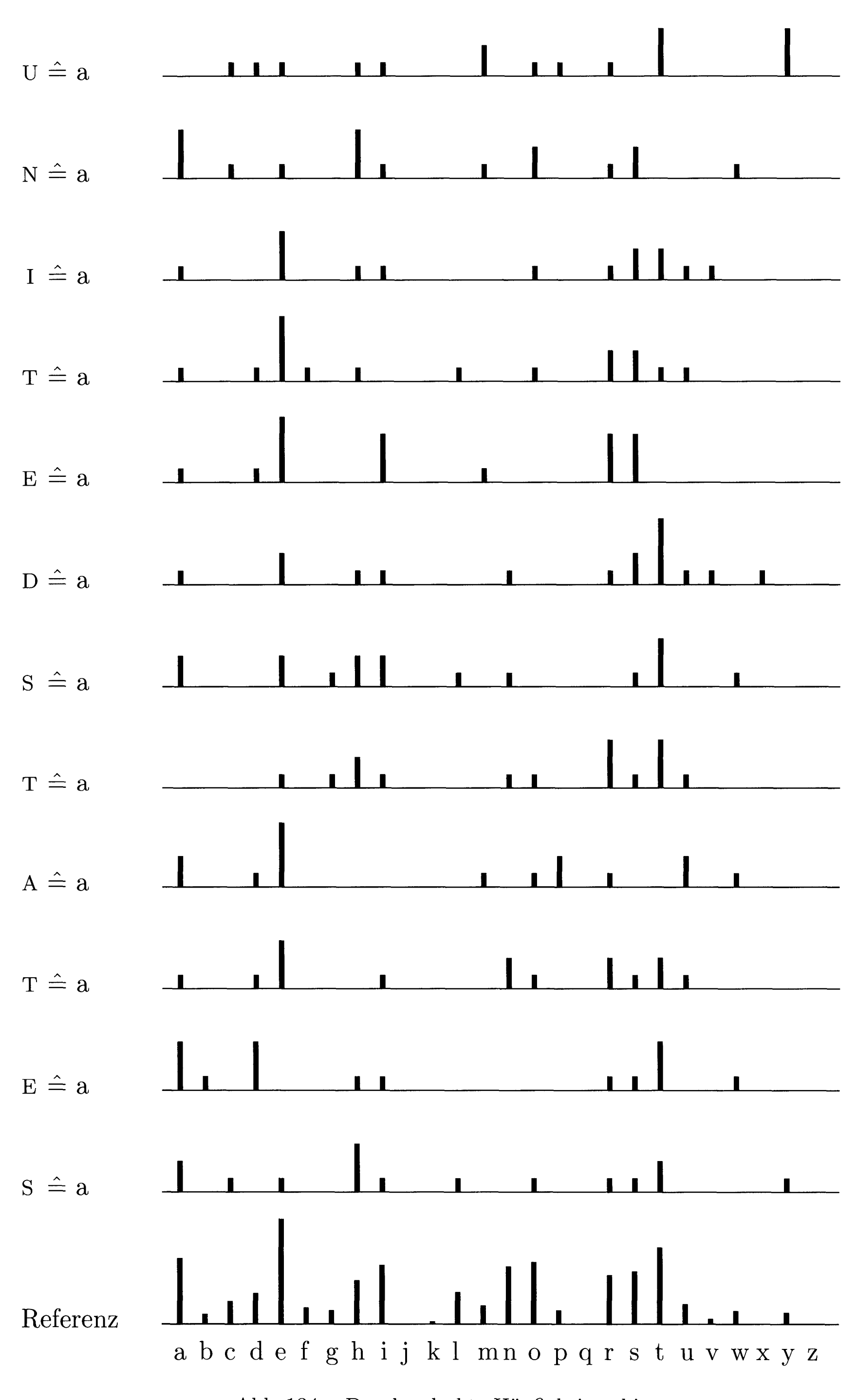


Abb. 134. Durchgedeckte Häufigkeitsgebirge

nete Verschiebung mit der Häufigkeitsverteilung des Englischen einigermaßen zur Deckung bringen (‚durchdecken') kann.

Allerdings führt die 11. Kolonne etwas in die Irre: /e/, der häufigste Buchstabe, kommt darin gar nicht vor. Allgemein kann man sagen, daß es bei so kleinen Zeichenmengen besser gelingt, zunächst die seltenen Buchstaben zur Deckung zu bringen. Immerhin geben dann die /e/ in der dritten, vierten, fünften, neunten und zehnten Kolonnen einen guten Anhaltspunkt.

Es ergibt sich, daß das Klartext-/a/ im ersten Alphabet U, im zweiten Alphabet N, im dritten Alphabet I, im vierten, im achten und im zehnten Alphabet T, im fünften und im elften Alphabet E, im sechsten Alphabet D, im siebten und im zwölften Alphabet S entspricht. Im neunten Alphabet entspricht dem Klartext-/a/ das A, diese Substitution ist die identische. Sie bei einem VIGÈNERE zu unterdrücken, wäre angesichts der dann möglichen negativen Mustersuche (14.1) ein Kunstfehler.

Zum Durchdecken hilft hier sicher auch, daß der Schlüssel den Buchstaben *T*, wie sich herausstellt, gleich dreimal – im vierten, im achten und im zehnten Alphabet – enthält. Mit anderen Worten, das Schlüsselwort ist

UNITEDSTATES

Das ist den Umständen nach durchaus sinnvoll, und die Entzifferung nach *Rohrbach*s strenger Forderung (13.3.1) mag damit, mit $d = 12$ als Periode des Schlüssels, als abgeschlossen gelten. Für Neugierige sei noch der entzifferte Text[1] wiedergegeben (Abb. 135).

m r a l e	x a n d e	r h o w i	s i t t h	a t t h e	m e s s e
n g e r a	r r i v e	s h e r e	a t t h e	s a m e t	i m e w i
t h t h e	s a t u r	d a y c o	u r i e r	a n d o t	h e r s a
t u r d a	y p a p e	r s w h e	n a c c o	r d i n g	t o t h e
d a t e i	t i s p u	b l i s h	e d t h r	e e d a y	s p r e v
i o u s i	s t h e f	a u l t w	i t h y o	u o r t h	e p o s t
m a s t e	r s				

Abb. 135. Klartext von *G. W. Kulp*

18.2 Chi-Test: Zurechtrücken gegen bekanntes Alphabet

Das Zurechtrücken des Alphabets „mit bloßem Auge" mag in Abb. 133 etwa bei der ersten oder bei der achten Kolonne schwierig erscheinen.

18.2.1 Rechnerische Methoden erweisen sich als ein schärferes Mittel; es bietet sich an, die Verschiebung einer bestimmten Kolonne gegen das Referenzalphabet zu prüfen durch Berechnung des *Chi*. Abb. 136 und Abb. 137 zeigen dies für das unverschobene und das geeignet verschobene Alphabet der ersten Kolonne mit /a/ entsprechend U.

[1] Die Entzifferung gelang *Brian J. Winkel* 1975, darüber berichtete zuerst *Martin Gardner* im SCIENTIFIC AMERICAN, August 1977.

0	1	1	0	0	0	2	0	1	1	0	1	0	
A	B	C	D	E	F	G	H	I	J	K	L	M	
8.04	1.54	3.06	3.99	12.51	2.30	1.96	5.49	7.26	0.16	0.67	4.14	2.53	
a	b	c	d	e	f	g	h	i	j	k	l	m	
3	0	0	0	0	3	0	0	0	1	1	1	0	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
7.09	7.60	2.00	0.11	6.12	6.54	9.25	2.71	0.99	1.92	0.19	1.73	0.09	64.81
n	o	p	q	r	s	t	u	v	w	x	y	z	

Abb. 136. *Chi* für Referenzalphabet gegen 1. Kolonne

0	0	1	1	1	0	0	1	1	0	0	0	2	
U	V	W	X	Y	Z	A	B	C	D	E	F	G	
8.04	1.54	3.06	3.99	12.51	2.30	1.96	5.49	7.26	0.16	0.67	4.14	2.53	
a	b	c	d	e	f	g	h	i	j	k	l	m	
0	1	1	0	1	0	3	0	0	0	0	3	0	
H	I	J	K	L	M	N	O	P	Q	R	S	T	
7.09	7.60	2.00	0.11	6.12	6.54	9.25	2.71	0.99	1.92	0.19	1.73	0.09	86.03
n	o	p	q	r	s	t	u	v	w	x	y	z	

Abb. 137. *Chi* für Referenzalphabet gegen 1. Kolonne, verschoben

Im ersten Fall (a $\hat{=}$ A) ergibt sich *Chi* zu 64.81/16 % = 4.05%; im zweiten Fall (a $\hat{=}$ U) erhält man den bedeutend größeren Wert 86.03/16 % = 5.37%. Daß sich neben a $\hat{=}$ U auch a $\hat{=}$ J und a $\hat{=}$ F gegenüber allen anderen Verschiebungen auszeichnet, zeigt sich in Tabelle 20. Diese drei Wahlmöglichkeiten sind exhaustiv weiterzubehandeln.

Jedenfalls ist gezeigt, daß und wie ein periodisches VIGENÈRE-System unter nicht zu ungünstigen Umständen mechanisch entziffert werden kann. Für ein Problem vom Umfang der Sache *Kulp vs. Poe* reicht die Unterstützung durch einen Arbeitsplatzrechner völlig aus.

18.2.2 Die Grundidee des Zurechtrückens gegen ein Referenzalphabet – sei es, im Fall von VIGENÈRE-Schritten, das Standardalphabet, sei es, im Fall von ALBERTI-Schritten, gegen ein in unbefugte Hände gefallenes permutiertes Alphabet als Referenzalphabet – findet sich, ohne rechnerische Bestimmung des *Chi*, schon früh. Es ist weithin üblich, Streifen mit dem Referenzalphabet zu verwenden, auf denen etwa die neun häufigsten Zeichen (im Englischen e t a o n i r s h) fett gedruckt oder rot geschrieben, bei maschinellen Lösungen im 2. Weltkrieg (z.B. *Witt*, *Rohrbach*) auch mit halbdurchsichtigem Papier oder mit Schwärzungen versehen sind; weiterhin die fünf seltensten Zeichen (im Englischen j k q x z) ganz fehlen. Stellt man dann eine Kolonne des Geheimtextes als Zeile ein, so muß sich der zugehörige Klartext – der allerdings im Periodenabstand zerrissen ist – in irgendeiner Zeile finden. Plausibel ist es, die „fetteste“ Zeile oder eine der fettesten zu nehmen, vorausgesetzt sie hat keines (oder kaum eines) der seltenen Zeichen. In Abb. 138 ist dies für die erste Kolonne G I Y L B N S N J W X C S N S G des

Alignment	*Chi*	
a $\hat{=}$ A	4.05%	
a $\hat{=}$ B	3.54%	
a $\hat{=}$ C	3.70%	
a $\hat{=}$ D	2.64%	
a $\hat{=}$ E	4.38%	
a $\hat{=}$ F	5.54%	⟵
a $\hat{=}$ G	4.07%	
a $\hat{=}$ H	2.97%	
a $\hat{=}$ I	2.98%	
a $\hat{=}$ J	5.13%	⟵
a $\hat{=}$ K	4.43%	
a $\hat{=}$ L	3.60%	
a $\hat{=}$ M	1.72%	
a $\hat{=}$ N	4.30%	
a $\hat{=}$ O	4.85%	
a $\hat{=}$ P	4.30%	
a $\hat{=}$ Q	3.00%	
a $\hat{=}$ R	2.77%	
a $\hat{=}$ S	4.71%	
a $\hat{=}$ T	3.59%	
a $\hat{=}$ U	5.37%	⟵
a $\hat{=}$ V	3.71%	
a $\hat{=}$ W	3.37%	
a $\hat{=}$ X	2.65%	
a $\hat{=}$ Y	4.18%	
a $\hat{=}$ Z	4.62%	

Tabelle 20.
Berechnete Werte von *Chi*
für Referenzalphabet gegen 1. Kolonne

in Abb. 128 behandelten Beispiels durchgeführt. Die mit a $\hat{=}$ U bezeichnete Verschiebung hebt sich deutlich hervor. Zwar hat die mit a $\hat{=}$ F bezeichnete Zeile sogar ein fettes Zeichen mehr, aber auch ein Handicap-x. Die Problematik der Entscheidung zwischen diesen beiden Schlüsseln *U* und *F* für die erste Kolonne tritt wie in Abb. 134 wieder auf. Die übrigen Zeilen fallen deutlich ab.

18.2.3 Wird auch für die zweite Kolonne die Verschiebung ermittelt, so kann man darauf hoffen, daß Bigrammhäufigkeiten die Entscheidung zwischen den beiden konkurrierenden Schlüsseln *U* und *F* erleichtern. Die Bestimmung der einzelnen Schlüsselbuchstaben stützt sich so gegenseitig.

18.2.4 Eine verwandte Methode benutzt einen Schieber oder eine Scheibe, genau dem Original entsprechend, also das Standardalphabet oder ein in unbefugte Hände gefallenes permutiertes Alphabet aufweisend. Die häufigen Klartextzeichen werden wieder fett geschrieben, die seltensten Zeichen fallen weg. Auf dem Lineal oder auf der Scheibe der Geheimtextzeichen werden die

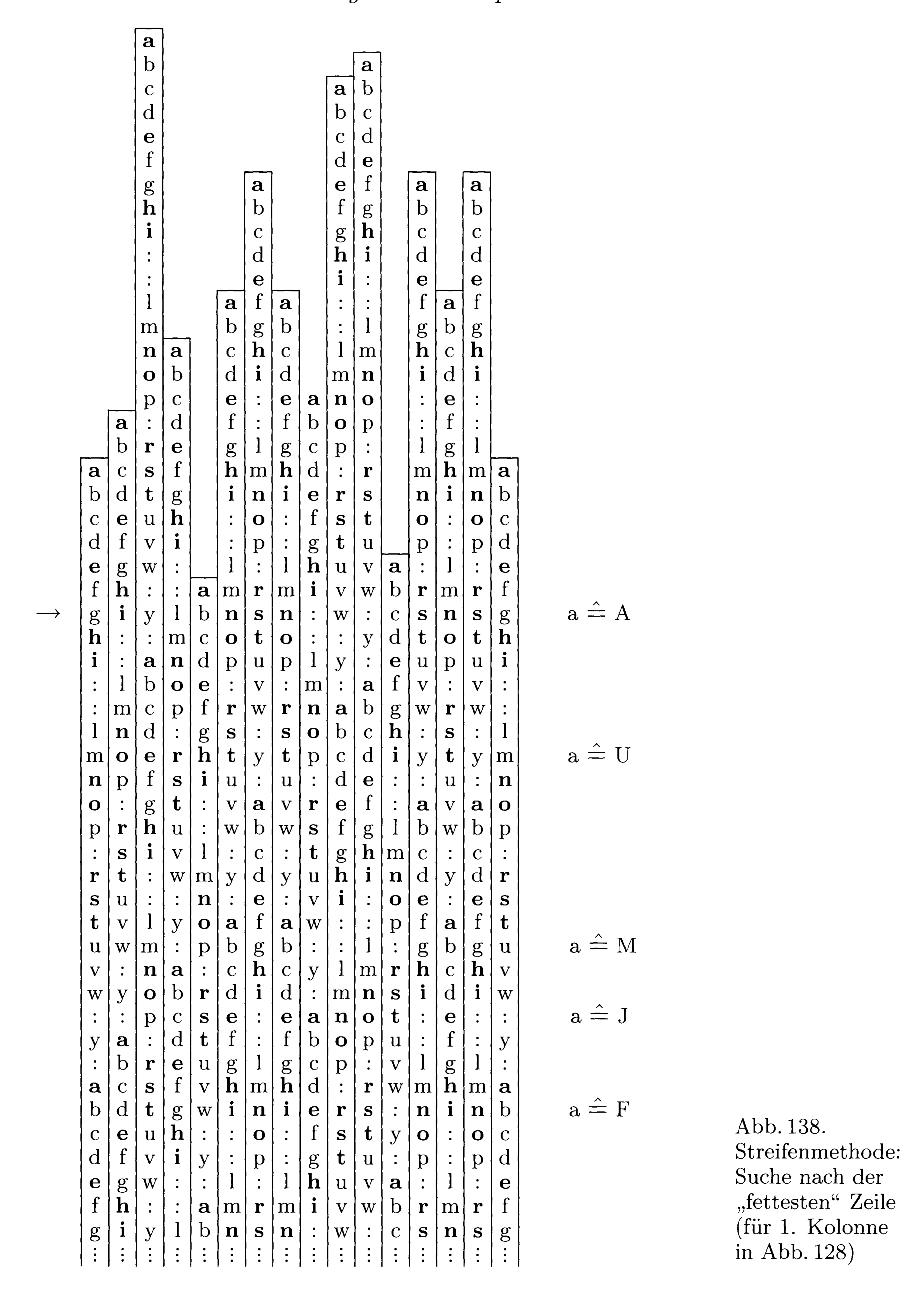


Abb. 138. Streifenmethode: Suche nach der „fettesten" Zeile (für 1. Kolonne in Abb. 128)

beobachteten Häufigkeiten notiert. Für die Buchstaben der Kolonne G I Y L B N S N J W X C S N S G zeigt Abb. 139 folgende Markierungen:

$$\mathrm{A}\ \bar{\mathrm{B}}\ \bar{\mathrm{C}}\ \mathrm{D}\ \mathrm{E}\ \mathrm{F}\ \bar{\bar{\bar{\mathrm{G}}}}\ \mathrm{H}\ \bar{\mathrm{I}}\ \bar{\mathrm{J}}\ \mathrm{K}\ \bar{\mathrm{L}}\ \mathrm{M}\ \bar{\bar{\bar{\bar{\mathrm{N}}}}}\ \mathrm{O}\ \mathrm{P}\ \mathrm{Q}\ \mathrm{R}\ \bar{\bar{\bar{\bar{\mathrm{S}}}}}\ \mathrm{T}\ \mathrm{U}\ \mathrm{V}\ \mathrm{W}\ \mathrm{X}\ \mathrm{Y}\ \mathrm{Z}\quad .$$

Man verschiebt nun die beiden Schieber oder Scheiben gegeneinander, bis man die „fetteste" Zuordnung hat. Für den Fall des Standardalphabets fällt diese Methode mit der unter 18.2.2 geschilderten zusammen.

a b c d e f g h i . . l m n o p . r s t u v w . y . a b c d e f g h i . . l m n o p . r s t u v w . y .

a ≙ U   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

a b c d e f g h i . . l m n o p . r s t u v w . y . a b c d e f g h i . . l m n o p . r s t u v w . y .

a ≙ F   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

a b c d e f g h i . . l m n o p . r s t u v w . y . a b c d e f g h i . . l m n o p . r s t u v w . y .

a ≙ M   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Abb. 139. Schieber für Entzifferung einer Kolonne
a ≙ U: gute, a ≙ F: ebenfalls gute, a ≙ M: schlechte Übereinstimmung

18.2.5 Nach diesem Prinzip kann man in allen Fällen vorgehen, in denen die Vorschrift bekannt ist, nach der aus einer Referenzsubstitution alle Substitutionen erhalten werden, also beispielsweise auch für ROTOR-Chiffrierschritte. Eine Tiefe von mindestens 6 bis 9 ist dabei wünschenswert, d.h. ein Geheimtext von 6 bis 9 Geheimtextzeichen pro zu bestimmendes Alphabet. Anders ausgedrückt: Um gegen diesen Angriff sicher zu sein, sollte der Klartext nicht länger als sechs mal die Schlüssellänge sein.

Im übrigen ist die Methode auch für eine polyalphabetische Chiffrierung mit beliebigen unabhängigen Alphabeten brauchbar, wenn – womit man nach *Kerckhoffs* und *Shannon* immer rechnen muß – alle Alphabete in unbefugte Hände gefallen sind, also etwa ein ganzer Zylinder M-94 oder ein ganzes Streifengerät CSP-642, oder bereits in Familien gruppiert sind (vgl. 14.3.6). Man braucht dann nur einen in der richtigen Periode durch Kolonnenbildung zerrissenen Teiltext gegen jedes einzelne Alphabet durchzuprobieren. Wiederum reicht dazu heute die Unterstützung durch einen Arbeitsplatzrechner völlig aus. Allerdings sind die zerrissenen Teiltexte oft zu kurz, um etwas Brauchbares zu ergeben. Normalerweise braucht man mindestens 40 oder 50 Geheimtextzeichen pro Schlüsselzeichen, um Erfolg zu haben.

18.3 Chi-Test: Gegenseitiges Zurechtrücken begleitender Alphabete

Ist das Referenzalphabet nicht das Standardalphabet, so verbleibt immer noch die Möglichkeit, die einzelnen begleitenden Alphabete gegenseitig zurechtzurücken und damit den polyalphabetisch chiffrierten Geheimtext zu ersetzen durch einen monoalphabetisch chiffrierten Geheimtext, der sodann nach den Methoden des 15. Kapitels zu brechen ist. Dieses Vorgehen ist auch brauchbar, falls das Referenzalphabet das Standardalphabet ist, wenn man das aber bei sehr kleinem Umfang des Geheimtextes nicht erkennt.

11	9	12	9	12	8	3	4	10	21	5	7	19	9	20	10	8	20	12	4	8	14	22	13	7	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Abb. 140. Häufigkeitsverteilung im Geheimtext 18.3.1

18.3.1 Nachfolgender Geheimtext (*Sinkov* 1968) hat die in Abb. 140 wiedergegebene Häufigkeitsverteilung, die mit ihrer Ausgeglichenheit nicht auf Monoalphabetizität hindeutet.

```
SWWJR GPRDN FMWJE XEWGR ZJQDN VJZRV
SZXOJ VWWRO VBHRM MOFDL IPAXV EZWUT
CZOZA AQQJL UPKZZ XUMJA PCZOE BAWZR
ZYKZI POFOL UOCRE NYKRI CAMOX IOORR
ZJKOL VWWJN VPKZA AFOCA MZOMR CJZDY
EJXEL XRFQI ZJCMA RJVWI DSWZX ASOTR
BJBZO QPXMI PDJVZ ZXHGQ SZFDQ FJZJR
BMWIC EZMWL MECVY VWZOX TWHSR UUBMT
NSJDW SSOOW CUNJY VJEWI PPFSL MOQVY
CVWRI SMMHW XMEJY NUZMV MXWCR NBRDE
SNB
```

Der *Phi*-Wert ist 4.56% und bestätigt diese Vermutung. Es finden sich neun Parallelstellen der Länge 3, allerdings keine längeren; die Abstände sind für

WWJ : $125 = 5 \cdot 5 \cdot 5$
RZJ : $100 = 2 \cdot 2 \cdot 5 \cdot 5$
JVW : $132 = 2 \cdot 2 \cdot 3 \cdot 11$
VWW : $90 = 2 \cdot 3 \cdot 3 \cdot 5$
CZO : $21 = 3 \cdot 7$
ZAA : $70 = 2 \cdot 5 \cdot 7$
PKZ : $60 = 2 \cdot 2 \cdot 3 \cdot 5$
ZZX : $121 = 11 \cdot 11$
CAM : $28 = 2 \cdot 2 \cdot 11$.

Die Kasiski-Untersuchung vermag nicht zwischen den möglichen Perioden 5 und 7 zu unterscheiden. Dies gelingt jedoch mit der kolonnenweisen *Phi*-Bestimmung nach *Kullback*: Für eine Anordnung in 7 Kolonnen erhält man den niedrigen Wert $Phi^{(7)} = 4.6\%$; für eine Anordnung in 5 Kolonnen ergibt sich jedoch ein Anhaltspunkt für Monoalphabetizität in jeder Kolonne: Abb. 141a zeigt dies sowohl hinsichtlich der wenig ausgeglichenen Häufigkeiten wie hinsichtlich der Bildung der ϕ_r-Werte, es resultiert $Phi^{(5)} = 6.47\%$. Jedoch scheint keine der monoalphabetisch chiffrierten Kolonnen ein verschobenes Häufigkeitsgebirge für das Englische oder eine andere geläufige Sprache aufzuweisen: Ein Blick voraus auf Abb. 141b zeigt dies, etwa für die erste Kolonne. Es ist also nicht an ein VIGENÈRE-System zu denken.

18.3.2 Zur Entzifferung jeder einzelnen Kolonne für sich ist die Textbasis zu schmal. Wenn es sich um ALBERTI-Schritte handeln würde, könnten die einzelnen, gegenüber einem bestimmten, aber unbekannten Referenzalphabet

1. Kolonne

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	4	5	1	3	2	1	0	2	0	0	0	5	4	0	4	1	1	6	1	3	6	0	4	0	5

$\phi_1 = 190$

2. Kolonne

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	2	1	1	2	1	0	0	0	10	0	0	4	1	5	6	1	1	4	0	4	1	5	2	2	6

$\phi_2 = 234$

3. Kolonne

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	3	3	0	2	5	0	3	0	2	5	0	4	1	6	0	3	2	0	0	0	1	11	3	0	6

$\phi_3 = 258$

4. Kolonne

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	0	2	7	1	0	2	1	1	8	0	0	5	0	7	0	1	7	2	1	1	3	3	1	0	7

$\phi_4 = 262$

5. Kolonne

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5	0	1	0	4	0	0	0	7	1	0	7	1	3	2	0	2	9	0	2	0	3	3	3	5	2

$\phi_5 = 240$

Abb. 141a. Häufigkeitsverteilung in fünf Kolonnen

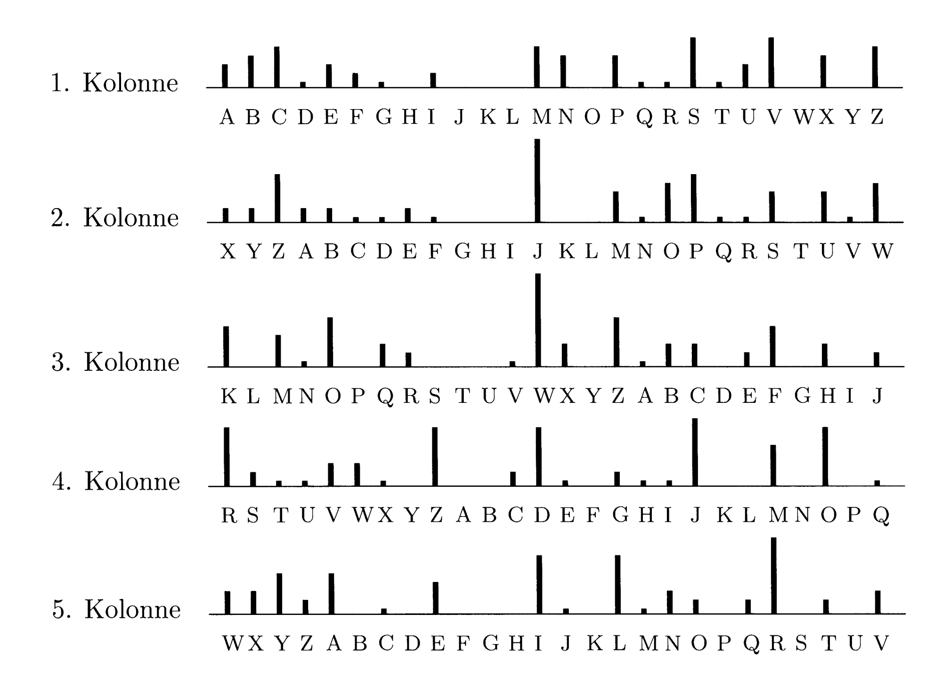


Abb. 141b. Durchgedecktete Häufigkeitsgebirge für fünf Kolonnen

verschobenen Alphabete gegenseitig durchgedeckt werden; dadurch entstünde ein reduzierter **Zwischentext**, der alle Kolonnen monoalphabetisch umfaßt, also eine wesentlich breitere Textbasis bietet und den Kontakt wieder herstellt. Das Ergebnis einer solchen Durchdeckung zeigt Abb. 141b. Zur Durchdeckung der i-ten mit der k-te Kolonne berechnet man für $q=0\ldots N{-}1$ das *Chi* der i-ten Kolonne gegen die um q Schritte zyklisch verschobene k-te Kolonne. Normalerweise hebt sich aus einer Reihe um κ_{R} schwankender Werte ein einziger, in der Nähe von κ_{S} liegender Wert heraus (Tabelle 21), das zugehörige q ergibt die zur Durchdeckung erforderliche Verschiebung.

Alignment	*Chi*	
$A^{(1)} \hat{=} A^{(2)}$	$158/61^2 = 4.25\%$	
$A^{(1)} \hat{=} B^{(2)}$	$129/61^2 = 3.47\%$	
$A^{(1)} \hat{=} C^{(2)}$	$161/61^2 = 4.33\%$	
$A^{(1)} \hat{=} D^{(2)}$	$122/61^2 = 3.28\%$	
$A^{(1)} \hat{=} E^{(2)}$	$139/61^2 = 3.74\%$	
$A^{(1)} \hat{=} F^{(2)}$	$136/61^2 = 3.65\%$	
$A^{(1)} \hat{=} G^{(2)}$	$100/61^2 = 2.69\%$	
$A^{(1)} \hat{=} H^{(2)}$	$169/61^2 = 4.54\%$	
$A^{(1)} \hat{=} I^{(2)}$	$126/61^2 = 3.39\%$	
$A^{(1)} \hat{=} J^{(2)}$	$124/61^2 = 3.33\%$	
$A^{(1)} \hat{=} K^{(2)}$	$187/61^2 = 5.03\%$	
$A^{(1)} \hat{=} L^{(2)}$	$87/61^2 = 2.34\%$	
$A^{(1)} \hat{=} M^{(2)}$	$161/61^2 = 4.33\%$	
$A^{(1)} \hat{=} N^{(2)}$	$138/61^2 = 3.71\%$	
$A^{(1)} \hat{=} O^{(2)}$	$161/61^2 = 4.33\%$	
$A^{(1)} \hat{=} P^{(2)}$	$138/61^2 = 3.71\%$	
$A^{(1)} \hat{=} Q^{(2)}$	$115/61^2 = 3.09\%$	
$A^{(1)} \hat{=} R^{(2)}$	$172/61^2 = 4.62\%$	
$A^{(1)} \hat{=} S^{(2)}$	$129/61^2 = 3.47\%$	
$A^{(1)} \hat{=} T^{(2)}$	$122/61^2 = 3.28\%$	
$A^{(1)} \hat{=} U^{(2)}$	$185/61^2 = 4.97\%$	
$A^{(1)} \hat{=} V^{(2)}$	$136/61^2 = 3.65\%$	
$A^{(1)} \hat{=} W^{(2)}$	$149/61^2 = 4.00\%$	
$A^{(1)} \hat{=} X^{(2)}$	$234/61^2 = 6.29\%$	$\longleftarrow$
$A^{(1)} \hat{=} Y^{(2)}$	$97/61^2 = 2.61\%$	
$A^{(1)} \hat{=} Z^{(2)}$	$152/61^2 = 4.08\%$	

Tabelle 21.
Berechnete Werte von *Chi* für erste Kolonne gegen zweite Kolonne

Sinkov gibt verschiedene Strategien des Zurechtrückens an: die kettenförmige mit einer Durchdeckung der 2. Kolonne gegen die 1., der 3. Kolonne gegen die 2., der 4. Kolonne gegen die 3., der 5. Kolonne gegen die 4. (usw.), womöglich auch zur Kontrolle ringförmig geschlossen; eine sternförmige mit einer Durchdeckung der 2. Kolonne gegen die 1., der 3. Kolonne gegen die 1., der 4. Kolonne gegen die 1., der 5. Kolonne gegen die 1. (usw.). Beide Strategien haben Vor- und Nachteile und sollten nicht gedankenlos verwendet werden.

Es kann vorkommen, daß sich nicht ein einziger *Chi*-Wert deutlich hervorhebt, wie es das Beispiel der Durchdeckung der 3. Kolonne gegen die 4. Kolonne zeigt (Tabelle 22): $A^{(3)} \hat{=} H^{(4)}$ und $A^{(3)} \hat{=} N^{(4)}$ unterscheiden sich kaum. Dann kann man zunächst eine andere Strategie verfolgen; bei zu kurzen Texten muß man womöglich zur Exhaustion unentschiedener Fälle greifen. In unserem Beispiel stellt sich heraus, daß $A^{(3)} \hat{=} H^{(4)}$ die richtige Zuordnung ist. Das ergibt schließlich die in Abb. 141b vorgenommene Durchdeckung.

Es ist also gezeigt, daß und wie ein periodisches ALBERTI-System unter nicht zu ungünstigen Umständen mechanisch bis auf eine höchstwahrscheinlich monoalphabetische Chiffre entziffert werden kann. Für ein Problem vom Umfang des Beispiels von *Sinkov* reicht die durch einen Arbeitsplatzrechner erzielte Unterstützung völlig aus.

18.3.3 Unter den in Abb. 141b bei vertikaler Ablesung auftretenden Wörtern AXKRW, BYLSX, CZMTY, DANUZ usw. fällt das Wort ROBIN auf. Es könnte das Schlüsselwort sein.

Alignment	*Chi*	
$A^{(3)} \hat{=} A^{(4)}$	$187/61^2 = 5.03\%$	
$A^{(3)} \hat{=} B^{(4)}$	$86/61^2 = 2.31\%$	
$A^{(3)} \hat{=} C^{(4)}$	$148/61^2 = 3.98\%$	
$A^{(3)} \hat{=} D^{(4)}$	$164/61^2 = 4.41\%$	
$A^{(3)} \hat{=} E^{(4)}$	$165/61^2 = 4.43\%$	
$A^{(3)} \hat{=} F^{(4)}$	$117/61^2 = 3.14\%$	
$A^{(3)} \hat{=} G^{(4)}$	$82/61^2 = 2.20\%$	
$A^{(3)} \hat{=} H^{(4)}$	$231/61^2 = 6.21\%$	$\longleftarrow$
$A^{(3)} \hat{=} I^{(4)}$	$122/61^2 = 3.28\%$	
$A^{(3)} \hat{=} J^{(4)}$	$110/61^2 = 2.96\%$	
$A^{(3)} \hat{=} K^{(4)}$	$143/61^2 = 3.84\%$	
$A^{(3)} \hat{=} L^{(4)}$	$109/61^2 = 2.85\%$	
$A^{(3)} \hat{=} M^{(4)}$	$150/61^2 = 4.03\%$	
$A^{(3)} \hat{=} N^{(4)}$	$228/61^2 = 6.13\%$	$\longleftarrow$
$A^{(3)} \hat{=} O^{(4)}$	$53/61^2 = 1.42\%$	
$A^{(3)} \hat{=} P^{(4)}$	$180/61^2 = 4.84\%$	
$A^{(3)} \hat{=} Q^{(4)}$	$146/61^2 = 3.92\%$	
$A^{(3)} \hat{=} R^{(4)}$	$103/61^2 = 2.77\%$	
$A^{(3)} \hat{=} S^{(4)}$	$206/61^2 = 5.54\%$	
$A^{(3)} \hat{=} T^{(4)}$	$108/61^2 = 2.90\%$	
$A^{(3)} \hat{=} U^{(4)}$	$124/61^2 = 3.33\%$	
$A^{(3)} \hat{=} V^{(4)}$	$190/61^2 = 5.11\%$	
$A^{(3)} \hat{=} W^{(4)}$	$113/61^2 = 3.04\%$	
$A^{(3)} \hat{=} X^{(4)}$	$124/61^2 = 3.33\%$	
$A^{(3)} \hat{=} Y^{(4)}$	$141/61^2 = 3.79\%$	
$A^{(3)} \hat{=} Z^{(4)}$	$124/61^2 = 3.33\%$	

Tabelle 22.
Berechnete Werte von *Chi* für dritte Kolonne gegen vierte Kolonne

18.4 Wiedergewinnung des Referenzalphabets

Die Herstellung des monoalphabetisch chiffrierten Zwischentextes geschieht durch systematische Umbezeichnung, wie sie Abb. 141b festlegt: Das Stück Geheimtext SWWJR erfährt folgende Behandlung:

$\mathrm{SWWJR} = \mathrm{S}^{(1)}\mathrm{W}^{(2)}\mathrm{W}^{(3)}\mathrm{J}^{(4)}\mathrm{R}^{(5)} = \mathrm{S}^{(1)}\mathrm{Z}^{(1)}\mathrm{M}^{(1)}\mathrm{S}^{(1)}\mathrm{V}^{(1)} = \mathrm{SZMSV}^{(1)}$

Insgesamt ergibt sich folgender Zwischentext, bezogen auf das Alphabet $^{(1)}$ der ersten Kolonne

SZMSV GSHMR FPMSI XHMPV ZMGMR VMPAZ
SCNXN VZMAS VEXAQ MRVMP ISQGZ ECMDX
CCEIE ATGSP USAID XXCSE PFPXI BDMIV
ZBAIM PRVXP URSAI NBAAM CDCXB IREAV
ZMAXP VZMSR VSAIE AIELE MCEVV CMPMC
EMNNP XUVZM ZMSVE RMLFM DVMIB AVECV
BMRIS QSNVM PGZED ZAXPU SCVMU FMPSV
BPMRG ECCFP MHSEC VZPXB TZXBV UXRVX
NVZMA SVEXA CXDSC VMUFM PSVBP MRGEC
CYMAM SPCQA XPUSC NXPVZ MAMLV NEHMI
SQR

Die Häufigkeitsverteilung, bezogen auf das Alphabet $^{(1)}$, lautet

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
20	11	21	7	19	6	7	4	14	0	0	3	40	9	0	23	5	13	25	2	8	29	0	20	1	16

Der Einstieg geschieht danach mit

$\mathrm{M}^{(1)} \hat{=}$ e , $\mathrm{V}^{(1)} \hat{=}$ t , $\mathrm{S}^{(1)} \hat{=}$ a .

Aus dem häufig vorkommenden Trigramm VZM $\hat{=}$ tZe erhält man

$\mathrm{Z}^{(1)} \hat{=}$ h .

Wenn man im freien Stil arbeitet, kann man aus dem Vorkommen von /heat/ großzügig auf das Vorkommen von /temperature/ schließen, tatsächlich hat die gegen Ende der siebten Zeile und in kurzem Abstand wieder auftretende Parallelstelle VMUFMPSVBP $\hat{=}$ teUFePatBP das verlangte Muster. Damit hat man bereits

$\mathrm{U}^{(1)} \hat{=}$ m , $\mathrm{F}^{(1)} \hat{=}$ p , $\mathrm{P}^{(1)} \hat{=}$ r , $\mathrm{B}^{(1)} \hat{=}$ u .

Zu Beginn der fünften Zeile findet sich

VZMAXPVZMSRV $\hat{=}$ theAXrtheaRt $\hat{=}$ thenortheast . Also

$\mathrm{A}^{(1)} \hat{=}$ n , $\mathrm{X}^{(1)} \hat{=}$ o , $\mathrm{R}^{(1)} \hat{=}$ s .

Die Entzifferung gelingt nun, da e t a o n r s h und einige seltenere Zeichen bestimmt sind, fast mühelos:

a h e a t G a H e s p r e a I o H e r t h e G e s t e r n h
a C N o N t h e n a t E o n Q e s t e r I a Q G h E C e D o
C C E I E n T G a r m a n I D o o C a E r p r o I u D e I t
h u n I e r s t o r m s a n I N u n n e C D C o u I s E n t
h e n o r t h e a s t a n I E n I E L E e C E t t C e r e C

```
E e N N r  o m t h e  h e a t E  s e L p e  D t e I u  n t E C t
u e s I a  Q a N t e  r G h E D  h n o r m  a C t e m  p e r a t
u r e s G  E C C p r  e H a E C  t h r o u  T h o u t  m o s t o
N t h e n  a t E o n  C o D a C  t e m p e  r a t u r  e s G E C
C Y e n e  a r C Q n  o r m a C  N o r t h  e n e L t  N E H e I
a Q s
```

Man ergänzt der Reihe nach
$G^{(1)} \hat{=} w$, $H^{(1)} \hat{=} v$, $I^{(1)} \hat{=} d$, $C^{(1)} \hat{=} l$, $N^{(1)} \hat{=} f$, $E^{(1)} \hat{=} i$,
$Q^{(1)} \hat{=} y$, $D^{(1)} \hat{=} c$, $T^{(1)} \hat{=} g$, $L^{(1)} \hat{=} x$, $Y^{(1)} \hat{=} b$.
und erhält einen Text, der offensichtlich Sinn macht:

```
a h e a t  w a v e s  p r e a d  o v e r t  h e w e s  t e r n h
a l f o f  t h e n a  t i o n y  e s t e r  d a y w h  i l e c o
l l i d i  n g w a r  m a n d c  o o l a i  r p r o d  u c e d t
h u n d e  r s t o r  m s a n d  f u n n e  l c l o u  d s i n t
h e n o r  t h e a s  t a n d i  n d i x i  e l i t t  l e r e l
i e f f r  o m t h e  h e a t i  s e x p e  c t e d u  n t i l t
u e s d a  y a f t e  r w h i c  h n o r m  a l t e m  p e r a t
u r e s w  i l l p r  e v a i l  t h r o u  g h o u t  m o s t o
f t h e n  a t i o n  l o c a l  t e m p e  r a t u r  e s w i l
l b e n e  a r l y n  o r m a l  f o r t h  e n e x t  f i v e d
a y s
```

Damit ist das Referenzalphabet bis auf eine Verschiebung wiedergewonnen. Über /j/, /k/, /q/, /z/ erfährt man nichts. Wenn man annehmen will, daß *ROBIN* tatsächlich der Schlüssel war, so lautet das zum Schlüsselbuchstaben *A* gehörige Referenzalphabet

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	
B	H	M	R	V	W	C	I	N	*	*	L	D	J	G	O	*	Y	A	E	K	Q	P	U	Z	*	,

zur Dechiffrierung umgeordnet

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
s	a	g	m	t	*	o	b	h	n	u	l	c	i	p	w	v	d	*	*	x	e	f	*	r	y	.

Jetzt scheint auch der „zweite Schlüssel“ zur Festlegung des permutierten Alphabets durch: Schreibt man die Alphabetsequenz in fünf Spalten

```
s o l v e
a b c d f
g h i * *
m n p * r
t u w x y
*          ,
```

so sieht man in der ersten Zeile das Kennwort /solve/ — das permutierte Alphabet ist also nach der in 3.2.5 beschriebenen Methode gebildet. Die Vervollständigung des Alphabets gelingt so auch:

s o l v e
a b c d f
g h i j k
m n p q r
t u w x y
z ,

das zum Schlüsselbuchstaben A gehörige Referenzalphabet lautet komplett

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	H	M	R	V	W	C	I	N	S	X	L	D	J	G	O	T	Y	A	E	K	Q	P	U	Z	F .

Damit ist im Sinn von *Rohrbach*s Forderung die Entzifferung beweiskräftig.

Die echten Parallelstellen RZJ und VWW werden zu /the/, PKZ wird zu /and/ entziffert; WWJ ist /hea/ in hea(t) bzw. (nort)hea(st) , ZAA ist /din/ in (colli)din(g) bzw. (an)d␣in . Es bestätigt sich auch das unwahrscheinliche Vorkommnis von vier unechten Parallelstellen.

18.5 Kerckhoffs' symétrie de position

Im Abschnitt 18.4 wurde aus methodischen Gründen nach einer Häufigkeitsanalyse im freien Stil verfahren. Häufig liegen aber Anhaltspunkte für wahrscheinliche Wörter vor und es besteht damit die Möglichkeit einer Mustererkennung. Dabei können für jedes der begleitenden Alphabete auch gewisse seltenere Klartext-Buchstaben entziffert werden. *Kerckhoffs* erkannte 1883, daß es in geeigneten Fällen möglich ist, eine solche Entzifferung von Zeichen einer gewissen Kolonne auch in andere, unbeteiligte Kolonnen zu übertragen. Er nannte die diesbezügliche, auf der Kommutativität der Addition in $\mathbb{Z}$ (vgl. 5. Kapitel) beruhende Eigenschaft der verschobenen Alphabete *symétrie de position*. Unter diesem Stichwort läuft insbesondere die nachfolgend an einem Originalbeispiel erläuterte Methode von *Kerckhoffs* .

18.5.1 Der Geheimtext sei

```
RBNBJ JHGTS PTABG JXZBG JICEM QAMUW
IVGAG NEIMW REZKZ SUABR RBPBJ CGYBG
JJMHE NPMUZ CHGWO UDCKO JKKBC PVPMJ
NPGKW PWADW CPBVM RBZBH JWZDN MEUAO
JFBMN KEXHZ AWMWK AQMTG LVGHC QBMWE
```

und eine Kasiski-Untersuchung der Bigramm-Parallelen RB, BJ, BG, RE, MJ, PQ nährt den Verdacht auf eine polyalphabetische Chiffrierung der Periode 5, möglicherweise mit verschobenen Alphabeten. Als ≪*mots probables*≫ des angeblich am 2. September 1882 in London aufgegebenen, an die Agence Havas in Le Caire (Kairo) gerichteten chiffrierten Telegramms kommen in Frage *Arabie, Wolseley*[2], *Suez, Ismaïlia, canal, général, soldats* . *Kerckhoffs* stellt zunächst durch Häufigkeitsanalyse fest, daß in der ersten Kolonne

[2] Lord Garnet J. Wolseley, Commander-in-Chief of the British Army.

J$^{(1)} \hat{=}$ e , in der zweiten und vierten B$^{(2)} \hat{=}$ B$^{(4)} \hat{=}$ e , in der dritten M$^{(3)} \hat{=}$ e , in der fünften Z$^{(5)} \hat{=}$ e sein könnte. Er findet damit

```
RBNBJ  JHGTS  PTABG  JXZBG  JICEM  QAMUW
*e*e*  e****  ***e*  e**e*  e****  **e**
```

was er unter einiger Überzeugungsarbeit als *le général Wolseley .....* deutet. Das führt zum Einstieg

```
RBNBJ  JHGTS  PTABG  JXZBG  JICEM  QAMUW
legen  eralw  olsel  ey*e*  e****  **e**
```

Damit ist auch G$^{(5)} \hat{=}$ l festgelegt und nach den Umständen liegt eine Fortsetzung mit *télégraphie* nahe:

```
RBNBJ  JHGTS  PTABG  JXZBG  JICEM  QAMUW
legen  eralw  olsel  eytel  egrap  hie**
```

Soweit die Vorgeschichte; die eigentümliche Methode setzt hier ein: Bisher ist (unter üblichem Vorbehalt) entziffert

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
(1)					J			Q				R			P											
(2)					B		I		A			T						H							X	
(3)	G				M		N											C	A	Z						
(4)	E				B							T														
(5)					Z							G		J		M							S			

Die *symétrie de position* kommt jetzt ins Spiel: Nicht nur müssen wegen B$^{(2)} \hat{=}$ B$^{(4)} \hat{=}$ e, T$^{(2)} \hat{=}$ T$^{(4)} \hat{=}$ l die zweite und die vierte Zeile gleich sein, was eine Ergänzung zu

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
(2)	E				B		I		A			T						H							X	
(4)	E				B		I		A			T						H							X	

erlaubt, es muß auch – da J in der ersten und in der fünften Zeile vorkommt und J$^{(1)} \hat{=}$ e , J$^{(5)} \hat{=}$ n = e+9 ist – die fünfte Zeile gegenüber der ersten um 9 Plätze nach rechts verschoben sein, was acht Chiffrenzeichen

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
(1)			G		J		M	Q				R		S	P							Z				
(5)					Z							G		J		M	Q				R		S	P		

festlegt. Aber auch die dritte und die fünfte Zeile sind etwa durch M$^{(3)} \hat{=}$ e , M$^{(5)} \hat{=}$ p = e+11 verbunden. Dies führt zu folgender Erweiterung auf elf Chiffrenzeichen:

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
(1)			G		J		M	Q	N			R		S	P					C	A	Z				
(3)	G		J		M	Q	N			R		S	P					C	A	Z						
(5)			C	A	Z							G		J		M	Q	N			R		S	P		

Schließlich ist die zweite und die dritte Zeile verbunden, etwa durch $\mathrm{A}^{(2)} \mathrel{\hat{=}} \mathrm{i}$, $\mathrm{A}^{(3)} \mathrel{\hat{=}} \mathrm{s} = \mathrm{i}+11$. Dies ergibt jetzt eine Verbindung aller fünf Alphabete unter Festlegung von insgesamt siebzehn Chiffrenzeichen:

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
(1)			G	H	J		M	Q	N		X	R	E	S	P		B		I	C	A	Z		T		
(2)	E	S	P		B		I	C	A	Z		T					G	H	J		M	Q	N		X	R
(3)	G	H	J		M	Q	N		X	R	E	S	P		B		I	C	A	Z		T				
(4)	E	S	P		B		I	C	A	Z		T					G	H	J		M	Q	N		X	R
(5)		I	C	A	Z		T					G	H	J		M	Q	N		X	R	E	S	P		B

Noch fehlen die Entzifferungen für D, F, K, L, O, U, V, W, Y . Man sollte aber mit 17 von 26 Zeichen erwarten, daß die weitere Entzifferung ohne Mühe läuft. In der Tat gibt das bisher Geleistete

```
RBNBJ  JHGTS  PTABG  JXZBG  JICEM  QAMUW
l e g e n  e r a l w  o l s e l  e y t e l  e g r a p  h i e * *

IVGAG  NEIMW  REZKZ  SUABR  RBPBJ  CGYBG
s * a i l  i a q u *  l a t t e  n * s e u  l e m e n  t q * e l

JJMHE  NPMUZ  CHGWO  UDCKO  JKKBC  PVPMJ
e s e r v  i c e * e  t r a * *  * * r * *  e * * e c  o m m u n
```

Mit dem wahrscheinlichen Wort *Ismaïlia* wird V, W festgelegt; offensichtliche Ausfüllungen geben U, Y ; liest man in der dritten Zeile *transports* heraus, so hat man auch D, K, O . F und L zieren sich am längsten, sie kommen erstmals in der fünften Zeile des Geheimtextes vor.

Aber in der Zwischenzeit zeigt sich ein besserer Weg, die Entzifferung zu Ende zu führen: Für die Bildung des Alphabets ist das Kennwort offenbar RESPUBLICA . Somit können die fünf Alphabete vervollständigt werden zu

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
(1)	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W
(2)	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R
(3)	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F
(4)	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R
(5)	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B

In der ersten Spalte unter dem Klartextbuchstaben /a/ scheint als Schlüsselwort DEGEL (frz. *dégel*, Tauwetter) auf, was Sinn ergibt.

Die vollständige Chiffriertabelle (*tabula recta*) zeigt Tabelle 23. Mit welcher Zeile man die Chiffriertabelle beginnen soll, bleibt übrigens offen; wir haben, *Kerckhoffs* folgend, diejenige Zeile genommen, in der das Kennwort am Ende steht. Das Schlüsselwort der Länge 5 ist dann *FRHRW* – aber der ‚wahre' Schlüssel ist wohl DEGEL; die erste Spalte der Matrix dient dann als Schlüsseleingang.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A
B	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z
C	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y
D	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T
E	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V
F	**D**	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W
G	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D
H	**G**	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F
I	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G
J	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H
K	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J
L	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K
M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M
N	N	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q
O	O	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N
P	X	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O
Q	R	E	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X
R	**E**	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R
S	S	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E
T	P	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S
U	U	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P
V	B	L	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U
W	**L**	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B
X	I	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L
Y	C	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I
Z	A	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C

Tabelle 23. Chiffriertabelle zum Beispiel von *Kerckhoffs*

Der Klartext lautet: "*Le général Wolseley télégraphie d'Ismaïlia qu'il attend seulement que le service de transports et de communication soit complètement organisé pour faire une nouvelle marche en v...*".

Zusammenfassend, die *symétrie de position* erlaubt "to extort more plaintext from a paucity of ciphertext" (*David Kahn*).

18.5.2 Der Flame *Auguste Kerckhoffs* (er hieß mit vollen Vornamen *Jean-Guillaume-Hubert-Victor-François-Alexandre*) wurde am 19. Januar 1835 in Nuth bei Limburg geboren. Er ging nahe Aachen zur Schule, studierte nach einem Englandaufenthalt in Lüttich, wurde Lehrer für moderne Sprachen und arbeitete als Reisesekretär, um sich schließlich in Melun, südöstlich Paris niederzulassen. Er wurde als etwas exzentrischer Mensch mit seiner Schulklasse nicht immer fertig, schlug sich aber wacker in philologischen Zirkeln. 1873 wurde er französischer Staatsbürger, 1873 bis 1876 studierte er an den Universitäten Bonn und Tübingen und promovierte. Nach einigen Umwegen bekam er 1878 eine Professur für deutsche Sprache an der École des Hautes Études Commerciales und an der École Arago zu Paris. 1892 schrieb er den Artikel *La cryptographie militaire* – wann, wo und wie er seine Vorstudien dazu durchführte, ist nicht bekannt. Der Beitrag von 64 Seiten im *Journal des Sciences militaires* vom Januar und vom Februar 1883 und der von *Kasiski*

sind jedenfalls die wichtigsten wissenschaftlichen kryptologischen Arbeiten des 19. Jahrhunderts.

Auguste Kerckhoffs wurde aber nicht wegen dieser Leistung weltberühmt, sondern wegen seines Eintretens für die Welthilfssprache VOLAPÜK, die um 1879 von *Johann Martin Schleyer* ersonnen worden war. *Kerckhoffs* wurde auf dem 2. VOLAPÜK-Weltkongreß in München 1887 zum *Dilekel* (‚Direktor') der Internationalen VOLAPÜK-Akademie ausgerufen. VOLAPÜK war eine Weile in Frankreich sehr geschätzt; wie ESPERANTO (*Ludwig Zamenhof* 1887) oder das von *Giuseppe Peano* 1903 vorgeschlagene INTERLINGUA hat es sich nicht durchsetzen können. *Kerckhoffs* erlebte den Niedergang des VOLAPÜK und starb als gebrochener Mann am 9. August 1903 in seinem Schweizer Urlaubsort.

18.5.3 Selbstverständlich ist die *symétrie de position* auch bei einer VIGENÈRE-Chiffrierung von Nutzen. Wir zeigen dies am Beispiel des Geheimtextes von *G. W. Kulp* (Abb. 115). Wir wollen jedoch zunächst nur annehmen, daß eine ALBERTI-Chiffrierung vorliegt, und daß einiges für die Periode 12 spricht. Dann gehen wir von einer Kolonnenbildung wie in Abb. 128 aus:

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
G	E	I	E	I	A	S	G	D	X	V	Z
I	J	Q	L	M	W	L	A	A	M	X	Z
Y	Z	M	L	W	H	F	Z	E	K	E	J
L	V	D	X	W	K	W	K	E	T	X	L
B	R	A	T	Q	H	L	B	M	X	A	A
N	U	B	A	I	V	S	M	U	K	H	S
S	P	W	N	V	L	W	K	A	G	H	G
N	U	M	K	W	D	L	N	R	W	E	Q
J	N	X	X	V	V	O	A	E	G	E	U
W	B	Z	W	M	Q	Y	M	O	M	L	W
X	N	B	X	M	W	A	L	P	N	F	D
C	F	P	X	H	W	Z	K	E	X	H	S
S	F	X	K	I	Y	A	H	U	L	M	K
N	U	M	Y	E	X	D	M	W	B	X	Z
S	B	C	H	V	W	Z	X	P	H	W	L
G	N	A	M	I	U	K					

und stellen fest, daß die in einer einzelnen Kolonne vorkommenden Chiffren häufig die Abstände 4 oder 7 oder 11 haben. Tatsächlich finden sich sogar sechs Tripel mit diesen drei Abständen:

	(3)	(4)	(6)	(7)	(10)	(12)
	B	M	W	L	M	L
+7						
	I	T	D	S	T	S
+4						
	M	X	H	W	X	W

Dieser Befund deutet auch bereits darauf hin, daß die 4. und die 10. Kolonne, sowie die 7. und die 12. Kolonne dem gleichen Schlüssel unterliegen.

Bei einem systematisch Vorgehen bildet man in jeder Kolonne paarweise die Differenzen zwischen den Chiffren und trägt sie in eine Tabelle ein. Diese ‚Differenzenmethode' ist nur eine Variante der *symétrie de position.* Sie liefert in unserem Fall ein Vorherrschen der Werte 4, 7, 11 (sowie der Komplemente 22, 19, 15) und damit einige weitere Fälle des Vorkommens der Differenzen 4 oder 7 oder 11. Es gibt auch „falsche" Differenzen: etwa in der 3. Spalte M und X.

Nun trägt man auch in den oben fehlenden Kolonnen diese Vorkommnisse noch ein:

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
	N		B	M		W	L	M		M	X	L
+7												
		N	I	T	E	D	S		A	T	E	S
+4												
	Y	R	M	X	I	H	W	X	E	X		W
(Verschiebung)	*0*	*19*	*14*	*25*	*10*	*9*	*24*	*25*	*6*	*25*	*10*	*24*

Die zur Deckung notwendigen Verschiebungen der einzelnen Kolonnen gegen die erste sind in einer Fußzeile eingetragen, sie ergeben einen Schlüssel. Den reduzierten, monoalphabetisch chiffrierten Zwischentext erhält man durch Subtraktion dieses Schlüssels, sein Anfang lautet demnach

G	L	U	F	Y	R	U	H	X	Y	L	B
I	Q	C	M	C	N	N	B	U	N	N	B
Y	G	Y	M	M	Y	H	A	Y	L	U	L
L	C	P	Y	M	B	Y	L	Y	U	N	N .

Die Entzifferung durch eine Häufigkeitsanalyse bietet kein Problem mehr, die Chiffrierung des Zwischentextes stellt sich, was wir bisher gar nicht ausgenützt haben, als eine CAESAR-Addition heraus mit U $\hat{=}$ a ; die Dechiffrierung erfolgt durch Weiterzählen um 6 . Der Anfang des Klartextes lautet also (s. a. 18.1.2)

m	r	a	l	e	x	a	n	d	e	r	h
o	w	i	s	i	t	t	h	a	t	t	h
e	m	e	s	s	e	n	g	e	r	a	r
r	i	v	e	s	h	e	r	e	a	t	t .

Die Differenzenmethode, die hier angeklungen ist, wird bei der Entzifferung von überchiffriertem Code im nächsten Abschnitt eine Rolle spielen. Sie ist von Häufigkeitsanalysen völlig frei. Würde man Häufigkeitsbetrachtungen bereits in die *symétrie de position* einbeziehen, so könnte man mutmaßen, daß in den obigen Tripeln die letzte Zeile, die am besten besetzt ist, dem /e/ entspricht und damit die erste Zeile dem /t/, die zweite dem /a/. Letzteres klärt auch auf, warum oben bereits das Schlüsselwort *UNITEDSTATES* durchschimmert.

18.6 Abstreifen einer Überchiffrierung: Differenzenmethode

Wir knüpfen an 18.3 an. Das gegenseitige Zurechtrücken begleitender Alphabete nimmt auf den Klartext gar keinen Bezug; er wird erst aus dem monoalphabetisch chiffrierten, hypothetischen Zwischentext (vgl. 18.4) wiedergewonnen. ALBERTI-Schritte sind nämlich Zusammensetzungen (9.1.1): monoalphabetische funktionale einfache Substitution, gefolgt von polyalphabetischen VIGENÈRE-Schritten.

18.6.1 Damit ist die Technik von 18.3 auch für überchiffrierten Code brauchbar, also für eine Komposition (9.2.1) von Codierung und nachfolgendem VIGENÈRE über $\mathbb{Z}_{26}$ (Buchstabencode) oder $\mathbb{Z}_{10}$ (Zifferncode). Letzteres hieß im englischen Jargon *"stripping off a numerical additive from enciphered code"* (*'encicode'*, der aus dem Codebuch geholte Code ist *'plain code'* oder *'placode'*); bei den deutschen Diensten sprach man von der „Subtraktion einer Überschlüsselungszahl".

Unter der Annahme einer gewissen Codelänge, beispielsweise 5 und einer gewissen Periode, beispielsweise 15, werden wieder Kolonnen von gleich überchiffrierten Codewörtern gebildet (‚Latten'). Häufig vorkommende Klartextwörter oder -phrasen führen in jeder dieser Latten zu Häufigkeitsunterschieden, bei genügend Material heben sich in jeder Latte gewisse Codegruppen heraus. Die reine Häufigkeitsuntersuchung, etwa durch Bildung von gegenseitigen *Chi*, mag erfolgreich sein; oft wird sie aber kein gegenseitiges Durchdecken zustande bringen.

18.6.2 Die *symétrie de position* hilft jedoch häufig weiter. Die sich in jeder Latte heraushebenden Codegruppen gehören genau dann zum selben Placode, wenn ihre Differenz *modulo* $\mathbb{Z}_{10}^5$ die Differenz der zu den betreffenden Latten gehörenden Überschlüsselungszahlen ergibt. Differenzen sind nach *Shannon* die *'residue classes'* der linearen polygraphischen Substitutionen.

Heben sich etwa in den ersten drei Latten die Codegruppen

(1)	(2)	(3)
47965	60597	27904
69451	34689	41537
11057	10056	26443

heraus, und gehören 47965 und 60597 zum selben *placode*, so gehören auch 11057 und 34689 zum selben *placode*, denn

$$47965 - 11057 \;=\; 60597 - 34689 \;=\; \mathbf{36918} \;\; \textit{modulo}\ \mathbb{Z}_{10}^5 \,.$$

Um solche Übereinstimmungen systematisch zu finden, bildet man für jede Latte die 3×3-Matrix der gegenseitigen Differenzen und findet auch **24633**:

	(1)			(2)			(3)	
00000	88514	**36918**	00000	**36918**	50541	00000	86477	25194
22596	00000	58404	74192	00000	**24633**	**24633**	00000	01561
74192	52606	00000	50569	86477	00000	85916	09549	00000

Es besteht also auch zwischen der zweiten und der dritten Latte die Beziehung *modulo* $\mathbb{Z}_{10}^5$

34689 − 10056 = 41537 − 27904 = **24633** .

Es ist ferner *modulo* $\mathbb{Z}_{10}^5$

47965 − 60597 = 87478 und 11057 − 34689 = 87478 , sowie
34689 − 41537 = 93152 und 10056 − 27904 = 93152 .

Reduziert man die zweite Latte relativ zur ersten, indem man überall die Differenz 87478 addiert, und die dritte Latte relativ zur zweiten, indem man überall die Differenzen 87478+93152=70520 addiert, so ergibt sich

	(1')	(2')	(3')
	47965	47965	97424
	69451	11057	11057
	11057	97424	96963
(Verschiebung)	*0*	*87478*	*70520*

Nunmehr sucht man in der ersten Latte nach Vorkommen – wenn auch seltener – von 97424 , ebenso in der (reduzierten) dritten Latte nach Vorkommen von 47965 ; im übrigen nach Vorkommen von 69451 , 97424 , 96963 . Im günstigsten Fall kann man so einige weitere gemeinsam vorkommende *placodes* „entdecken“.

18.6.3 Dieses Vorgehen erfordert umfangreiche rechnerische Arbeit, und es ist verständlich, daß man schon in den zwanziger Jahren des 20. Jhs. maschinelle Unterstützung für das Durchdecken suchte. Damals boten sich Lochkartenanlagen an, und insbesondere im 2. Weltkrieg setzten Briten (J. Tiltman, Sept. 1939), Amerikaner (R. J. Fabian, Nov. 1940) und Deutsche auf solche Hilfen.

Es wurden auch Spezialgeräte gebaut, so in der Chiffrierabteilung des Oberkommandos der Wehrmacht. Das „Differenzenrechengerät“ verarbeitete die auf Lochstreifen gestanzten Codegruppen über mechanische Abtaster und Relaisschaltungen; es lieferte pro Sekunde 7 Differenzenbildungen fünfstelliger Codegruppen und registrierte sie über eine Schreibmaschine. Es war damit fünf- bis zehnmal schneller als ein menschlicher Auswerter in der Spitze.

Zur Feststellung der am häufigsten auftretenden *placodes* wurden sowohl in der Abteilung *Chi* des Oberkommandos der Wehrmacht wie im Sonderdienst Dahlem des Auswärtigen Amtes mit Lichtmessung arbeitende Analoggeräte (für Tetragramme) eingesetzt. Auch für die Reduktion, die Subtraktion einer Konstanten von allen Codegruppen einer Latte bei bereits bekannter relativer Basis, wurden während des 2. Weltkriegs von *Ernst Witt* Spezialgeräte gebaut, die optisch arbeiteten.

Über einschlägige Spezialgeräte bei den Allierten des 2. Weltkriegs ist wenig bekannt. Die in *Bletchley Park* gebauten, angeblich speziell gegen die Fernschreib-Chiffriermaschine SZ 42 (‚Schlüsselzusatz‘) von LORENZ (Deckname TUNNY) gerichteten und einigermaßen universellen Geräte wie HEATH ROBINSON und COLOSSUS behandelten, könnte man sagen, binäre Additive.

In den USA hat es, wenn man *Burke* folgt, bis Kriegsende keine dem britischen COLOSSUS vergleichbare erfolgreiche Entwicklung gegeben. Auf der Stufe von HEATH ROBINSON standen die mit photoelektrischer Abtastung arbeitenden Geräte COPPERHEAD von 1943, die gegen japanische überchiffrierte Codes gerichtet waren. Am ehesten mit der deutschen Entwicklung zu vergleichen ist ein von Eastman für die Navy gebautes, mit Lichtmessung arbeitendes Gerät von 1942 (genannt TESSIE), das zum Auffinden von bestimmten vierstelligen Codegruppen (Tetragrammen) zwecks Abstreifen einer Überchiffrierung diente und sowohl gegen japanische Flottencodes wie gegen das deutsche „Kurzsignalbuch“gerichtet war, dessen Entzifferung vorzügliche ‘cribs’ für die Entzifferung der ENIGMA lieferte.

18.7 Entziffern des Codes

Schlußendlich verbleibt natürlich das Entziffern des nach dem Abstreifen der Überchiffrierung erhaltenen Zwischentextes, die Rekonstruktion des Codes (engl. *book-building*). Er ist gegenüber dem *placode* um eine Konstante verschoben, aber das spielt für die aufzubringende, hauptsächlich philologische Arbeit keine Rolle. Die Arbeit wird sehr erleichtert, wenn es sich um einen einteiligen Code (4.4.2) handelt. Dann liegt nämlich für ein Codewort, das lexikographisch zwischen zwei Codewörtern mit schon festgestellten Klartextwörtern liegt, das zugehörige Klartextwort zwischen diesen zwei Klartextwörtern. Im übrigen hat hier die Phantasie, noch mehr aber auch die Gestalterkennung, ein reiches Betätigungsfeld.

Um eine systematische Behandlung der philologischen Entzifferung von Codes hat sich erstmals (1892) *Paul Louis Eugène Valério* bemüht.

18.8 Rekonstruktion des Kennwortes

Der Vorteil begleitender Alphabete, daß sie sich aus einem einzigen Referenzalphabet ergeben, würde dem „eiligen“ Chiffrierer wenig nützen, wenn er sich nicht auch das Referenzalphabet leicht merken oder ableiten kann. Dazu dienen (vgl. 3.2.5) Kennwörter oder -sätze. Sie wiederzufinden, gibt dem unberufenen Entzifferer nicht nur zusätzliche Sicherheit, sondern kann methodisch genutzt werden — Merkwörter, also „memorierbare“ Kennwörter, sind eine Schwachstelle.

18.8.1 Zunächst wie ein Zaubertrick mutet folgendes Beispiel von *Friedman* (1917) an: Das Referenzalphabet sei

a b c d e f g h i j k l m n o p q r s t u v w x y z
N T U V P W X J F Y Z D K Q C A B O G R L I S H M E

es ist zyklisch mit dem Zyklus

(a n q b t r o c u l d v i f w s g x h j y m k z e p) .

Man bildet nun – etwa von a ausgehend – die Potenzen der Substitution N Q B T R O C U L D V I F . . . E P A und schreibt, zyklisch geschlossen, Folgen mit Abständen von 1, von 3, von 5, usw., also

N Q B T R O C U L D V I F W S G X . . . ,
N * * Q * * B * * T * * R * * O * . . . ,
N * * * * Q * * * * B * * * * T * . . . ,

Das ergibt insgesamt

1 N Q B T R O C U L D V I F W S G X H J Y M K Z E P A ;
3 N D J Q V Y B I M T F K R W Z O S P C G E U X A L H ;
5 N K X I C Q Z H F U B P J W L T E Y S D R A M G V O ;
7 N G R Y L P F Q X O M D E W B H C K V A S T J U Z I ;
9 N T C D F G J K P Q R U V W X Y Z A B O L I S H M E usw.

und liefert beim Abstand 9 eine Folge, die bereits ein Kennwort erscheinen läßt. Nimmt man nun klartextseitig die um neun Plätze nach rechts verschobene Folge, so ergibt sich folgende Substitution:

a b o l i s h m e n t c d f g j k p q r u v w x y z
9 N T C D F G J K P Q R U V W X Y Z A B O L I S H M E .

Man erhält durch Umordnung das obenstehende Ausgangsalphabet, das tatsächlich gewonnen worden ist durch neunfache Potenzierung eines Zyklus mit dem memorierbaren Kennwort *abolishment*:

(a b o l i s h m e n t c d f g j k p q r u v w x y z) .

Der Zaubertrick wird verständlicher, wenn man bedenkt, daß auch für die anderen Abstände sich solcherart ein Alphabet ergibt, aus dem man das Ausgangsalphabet durch Umordnung zurückerhält; etwa für den Abstand 7

a s t j u z i n g r y l e f q x o m d p w b h c k v
7 N G R Y L E F Q X O M D P W B H C K V A S T J U Z I ,

wobei zwar kein vernünftiges Kennwort auftaucht; oder mit dem Abstand 1:

a n q b t r o c u l d v i f w s g x h j y m k z e p
1 N Q B T R O C U L D V I F W S G X H J Y M K Z E P A .

Tatsächlich rekonstruiert die dritte Potenz dieser Substitution das Kennwort, da $3 \times 9 = 1$ *modulo* 26 .

18.8.2 *W. F. Friedman* hat auch angegeben (1918), wie man für den sehr allgemeinen Fall (3.2.5) eines mittels Kennwörtern für die Klartext- und für die Geheimtext-Seite konstruierten ALBERTI-Chiffriersystems die Kennwörter wiederauffinden kann. Wir werden darauf in 19.5.3 zurückkommen.

19 Kompromittierung

"The quality of a machine
depends largely on its use."

Boris Hagelin

Unter den im 11. Kapitel aufgeführten Chiffrierfehlern gehören Kompromittierungen zu den schlimmsten, denn sie eröffnen sogar methodische Angriffsmöglichkeiten. Die Klartext-Geheimtext-Kompromittierung wurde schon in 14.6 diskutiert. Nunmehr sollen die weniger auffälligen Fälle der Klartext-Klartext-Kompromittierung und der Geheimtext-Geheimtext-Kompromittierung behandelt werden.

19.1 Kerckhoffs' Superimposition

Polyalphabetische Chiffrierung mit periodischem Schlüssel bietet – selbst bei unbekannten unabhängigen Alphabeten – keine Sicherheit gegen unbefugte Entzifferung: Die Periode ist nach den Methoden des 16. Kapitels feststellbar, und dies erlaubt die Bildung von Kolonnen oder Latten jeweils monoalphabetisch chiffrierten Textes – allerdings zerrissenen Textes, der nur mit der Einzelzeichenhäufigkeit (Kapitel 15) angepackt werden kann, und oft zu kurz ist, wie schon in 18.2.5 und 18.3.2 angesprochen wurde.

Aber auch wenn der Schlüssel nicht periodisch ist, oder jedenfalls so lang, daß er länger ist als die Nachricht, besteht die gleiche Einbruchsmöglichkeit, sofern mehrere Klartexte mit dem selben Schlüssel chiffriert werden: Diese Klartext-Klartext-Kompromittierung des Schlüssels erlaubt bei **phasenrichtiger Überlagerung** (**Superimposition**) ebenfalls die Bildung von Kolonnen oder ‚Latten' jeweils monoalphabetisch chiffrierten, zerrissenen Textes („Tiefe des Materials", engl. '*building of a depth*'). *Kerckhoffs* beschäftigte sich 1883 in seiner schon für die *symétrie de position* genannten Arbeit mit diesem Fall (frz. *superimposition*, engl. *superimposition*). Selbstverständlich ist die Superimposition nur brauchbar, wenn genügend viele Nachrichten betroffen sind, aber dies ist gerade beim Einsatz von Chiffriermaschinen häufig genug der Fall: logistische Probleme der Schlüsselzuweisung und -verwaltung führen dazu. *John H. Tiltman* gelang es, auf diese Weise die von der Deutschen Reichsbahn im 2. Weltkrieg zur Übermittlung von Fahrplänen benutzte ältere ENIGMA ohne Steckerbrett (Reichsbahn-ENIGMA, britischer Deckname *rocket*) zu brechen.

Klar ist, daß auch die periodische Verwendung eines kurzen Schlüssels, die zu mehrmaliger Wiederholung führt, eine Klartext-Klartext-Kompromittierung darstellt – weil das aber recht üblich war, hat man es selten so genannt. Anders gesagt: Technisch ist die Anordnung eines periodisch chiffrierten Geheimtextes in Kolonnen nach der Periode, die *Kasiski* schon angepriesen hatte, ebenfalls eine phasenrichtige Überlagerung, eine Superimposition.

19.1.1 *Kerckhoffs* gibt folgendes einfaches (und recht günstig gelagertes) Beispiel einer Superimposition von dreizehn chiffrierten Texten (Chiffrierfehler, die ihm unterlaufen sind, sind bereinigt)

	1 2 3 4 5	6 7 8 9 10	11 12 13 14 15	16 17 18 19 20	21 22 23 24 25	26 27 28 29
(i)	U H Y B R	J I M B C	F A M M F	J H D M R	I Q	
(ii)	U H W P R	B Q L K I	B L W R E	J R B K L	H I X B Q	E X H M
(iii)	I E W H C	H Q K Q M	T M V G J	J E D Z V	A	
(iv)	U W V R R	H I K M C	W W R G H	D C X S R	Q H	
(v)	U H S H A	H K S V C	J W Z V X	J Y N D M	Q Q N	
(vi)	Y H V H M	A G Q K C	W X P V I	H H W L Z	V L T H V	
(vii)	L H V H A	A G R L P	F M S O H	I P W Z Z	J E L Q R	B W
(viii)	S W U I R	X I C J U	F S H G W	R S Z B A	A L	
(ix)	U H W H V	A Y U L C	J W O U K	D E B K Q		
(x)	Y W X H Y	H B A L G	B V P S W	I W W J R	R H	
(xi)	W Q R E X	B I E N H	M V Y M H	S I Y M		
(xii)	S W U H D	H P J J C	K X G M H	L		
(xiii)	G Q V Q R	V O T Q Q	S P W R			

Er beginnt mit Feststellungen wie, daß der Häufigkeit nach vermutlich $H^{(2)} \hat{=}$ e, $H^{(4)} \hat{=}$e, $R^{(5)} \hat{=}$ e, $H^{(6)} \hat{=}$ e, $I^{(7)} \hat{=}$ e, $L^{(9)} \hat{=}$ e, $C^{(10)} \hat{=}$ e, und daß somit vermutlich die zweite, vierte und sechste Stelle dem selben Alphabet unterliegen (klugerweise nimmt er nicht $U^{(1)} \hat{=}$ e an).

Die vierte Nachricht hätte dann die Entzifferung (iv) ∗∗∗∗eee∗∗..... , was nach einem Wort suchen läßt, das mit ée endet; l' armée wäre passend: (iv) larmeeee∗∗..... . Die fünfte Nachricht mit (v) le∗e∗e∗∗∗..... läßt auf (v) legeneral..... schließen. Die sechste Nachricht bietet dann bereits (vi) ∗ere∗v∗∗∗....., was (vi) serezvous..... oder (vi) ferezvous..... sein könnte. Die siebte Nachricht mit (vii) ∗erenvo∗e∗..... deutet *Kerckhoffs* einigermaßen überzeugend mit (vii) nerenvoyez..... . Dann wendet er sich den weiteren Nachrichten zu.

Superimposition ist als methodische Idee auch für den Fall unabhängiger Alphabete geeignet. Sofern die Anzahl verwendeter verschiedener Alphabete nicht über gute zwei Dutzend hinausgeht, etwa bei Bezeichnung durch Buchstaben, kommen bei nicht allzukurzen Nachrichten jeweils mehrere dieser Alphabete vor, die sich durch gleiche Häufigkeitsmerkmale verraten; die effektive Tiefe des Materials wird dadurch vervielfacht. Stammt der Schlüssel aus einem Text etwa in deutscher Sprache, so ist im Durchschnitt jedes sechste Schlüsselzeichen ein E und damit jedes sechste Alphabet das selbe.

19.1.2 Im vorliegenden Fall würde die Entzifferung trotzdem weiterhin mühevolle philologische Kleinarbeit sein, würde *Kerckhoffs* nicht die zusätzliche Annahme machen, daß die Alphabete nur gegenseitig verschoben sind und daß die *symétrie de position*, der Kernpunkt seiner Arbeit, herangezogen werden kann. Damit läuft dann alles wie am Schnürchen; einige der entzifferten Nachrichten (das Umfeld ist Nordafrika) lauten:

(i)	leprefetdepoliceestici	*≪le préfet de police est ici≫*
(ii)	lespertesdelennemisontgrandes	*≪les pertes de l' ennemi sont grandes≫*
(iii)	onsemetsurladefensive	*≪on se met sur la défensive≫*
(iv)	larmeeestentreeaucaire	*≪l' armée est entrée au Caire≫*
(v)	legeneralestaalexandrie	*≪le général est à Alexandrie≫*
(vi)	serezvousenetatderesister	*≪serez vous en état de résister≫*
(vii)	nerenvoyezpaslesprisonniers	*≪ne renvoyez pas les prisonniers≫* .

Es stellt sich heraus, daß *Kerckhoffs* dabei das gleiche ALBERTI-Alphabet verwendet wie in 18.5.1; der Schlüssel ist periodisch und läßt sich mit der Chiffriertabelle von Tabelle 23 rekonstruieren zu

$$JEMEMETSSURLADEFENSIVE \; .$$

19.2 Superimposition für Chiffrierungen mit einer Schlüsselgruppe

Selbst der (von *Kerckhoffs* nicht behandelte) Extremfall einer Superimposition von nur *zwei* Chiffraten, die mit dem selben Schlüssel erzielt wurden, ist unter günstigen Umständen nicht hoffnungslos.

19.2.1 Es sei angenommen, das Chiffrierschritt-System sei nicht nur injektiv und definal, d.h. zu jedem Chiffrierschritt $\chi_s : V^{(n)} \dashrightarrow W^{(m)}$ existiert ein Dechiffrierschritt $\chi_s^{-1} : W^{(m)} \dashrightarrow V^{(n)}$:

(*) $$\chi_s^{-1}(\chi_s(p)) = p \;\text{ für alle }\; p \in V^{(n)},$$

sondern der Einfachheit halber auch (2.6.2) eindeutig und surjektiv:

(**) $$\chi_s(\chi_s^{-1}(c)) = c \;\text{ für alle }\; c \in W^{(m)} .$$

Dann ist $|V^{(n)}| = |W^{(m)}|$. In diesem Fall liegt es nahe, Klartextzeichen und Geheimtextzeichen zu identifizieren, also $n = m$, $V \doteqdot W$ zu setzen, und den endomorphen Fall $\chi_s : V^n \longleftrightarrow V^n$ anzunehmen. $M \subseteq V^n \times V^n$ sei das Chiffrierschritt-System, $|V|$ sei N. M ist auch die Schlüsselmenge, wenn die Abbildung der Schlüsselmenge auf die Chiffrierschritte (2.6) injektiv ist.

Wichtig ist nun die Annahme, das Chiffrierschritt-System M sei **abgeschlossen**: Die Zusammensetzung zweier Chiffrierschritte $\chi_s \in M$, $\chi_t \in M$ gehöre wieder der Menge M an: $\chi_s(\chi_t(p)) = \chi_{s \bullet t}(p)$, wodurch $s \bullet t$ eindeutig definiert ist.

Die Zusammensetzung ist assoziativ: $\chi_{r \bullet s}(\chi_t(p)) = \chi_r(\chi_{s \bullet t}(p))$. Da auch jeder Chiffrierschritt ein Inverses $\chi_s^{-1} \in M$ besitzt, bilden die Chiffrierschritte eine Gruppe, die **Schlüsselgruppe** M. $\chi_{s^{-1}}(p)$ ist durch $\chi_s^{-1}(p)$ definiert.

Die Gruppe kann trivialerweise einelementig sein: $M = \{\text{id}\}$, sie kann auch N^n Elemente besitzen, etwa $M = \{\text{id}, \chi, \chi^2, \chi^3, \ldots \chi^{N^n-1}, \}$, wo χ zyklisch ist; oder gar (maximal) $(N^n)!$ Elemente haben: $M \doteqdot V^n \longleftrightarrow V^n$.

Nun seien $c' = (c'_1, c'_2, c'_3, \ldots)$ und $c'' = (c''_1, c''_2, c''_3, \ldots)$ zwei Geheimtexte, die aus den zwei Klartexten $p' = (p'_1, p'_2, p'_3, \ldots)$ und $p'' = (p''_1, p''_2, p''_3, \ldots)$ mit dem selben Schlüssel $k = (k_1, k_2, k_3, \ldots)$ hervorgegangen sind:

$$c'_i = \chi_{k_i}(p'_i) \ , \quad c''_i = \chi_{k_i}(p''_i) \ .$$

Es sei weiterhin angenommen, daß die Schlüsselgruppe M *transitiv* ist (14.3.4): Dann existiert ein Zeichen $a \in V^n$ derart, daß für jedes Zeichen $y \in V^n$ ein Chiffrierschritt $\chi_t \in M$ existiert mit $y = \chi_t(a)$. Damit ist auch die Anzahl der Schlüssel nicht kleiner als die Mächtigkeit des Alphabets V^n, $|M| \geq N^n$, und es kann jedem Zeichen aus V^n injektiv ein Schlüssel – vielleicht auch mehrere – zugeordnet werden.

Handelt es sich gar um ein Shannonsches Chiffrierschritt-System (2.6.4), so ist der Schlüssel k_i durch das Klartextzeichen p_i und das Geheimtextzeichen c_i eindeutig bestimmt;[1] es ist $|M| \leq N^n$ und damit $|M| = N^n$.

Die obige Zuordnung ist somit eineindeutig; wir haben ein **transitives Shannonsches Chiffrierschritt-System** mit einem lateinischen Quadrat als Chiffriertabelle. Eine Identifizierung der Schlüssel und der Zeichen gemäß $s = \chi_s(a)$ ergibt $s \bullet t = \chi_{s \bullet t}(a) = \chi_s(\chi_t(a)) = \chi_s(t)$ und somit

$$\chi_s(p) = s \bullet p \ , \quad \chi_{s \bullet t}(p) = \chi_{\chi_s(t)}(p) \ .$$

Ferner gilt

$$\chi_{s^{-1}}(c) = s^{-1} \bullet c = \chi_s^{-1}(c) \, .$$

Damit hat es einen Sinn, von $\chi_{c'_i}^{-1}(c''_i)$, dem mit dem Geheimtextzeichen c'_i als Schlüssel dechiffrierten phasengleichen Geheimtextzeichen c''_i zu sprechen. Eine einfache Rechnung ergibt das wichtige Resultat: Unter den angegebenen Bedingungen hebt sich in $\chi_{c'_i}^{-1}(c''_i)$ der Schlüssel heraus, genauer: es ist

$$\chi_{c'_i}^{-1}(c''_i) = \chi_{p'_i}^{-1}(p''_i) \ .$$

19.2.2 Für endomorphe Shannonsche Chiffrierungen mit einer transitiven Schlüsselgruppe bildet man also die **Differenz** $d_i \stackrel{\text{def}}{=} \chi_{c'_i}^{-1}(c''_i)$ und sucht zwei Klartexte p'_i, p''_i mit $\chi_{p'_i}^{-1}(p''_i) = d_i$. Dies kann in einem Zick-Zack-Wechselspiel wie in (14.4.3) versucht werden; Eindeutigkeit erfordert zwei Klartexte, deren jeder eine Redundanz (12.6, Fußnote 8) von mindestens 50% hat.

---

[1] Im allgemeinen braucht der Schlüssel k_i durch p_i und c_i gar nicht eindeutig bestimmt zu sein. Allerdings kann man ihn im extremen Fall $V \doteqdot Z_2$, $n = 1$ allein schon aus den einzelnen $c_i = \chi_{k_i}(p_i)$ rekonstruieren: Es gibt in diesem Falle nur die zwei Chiffrierschritte (8.3.1) der Identität O und der Involution L; für $p_i = c_i$ ist $k_i \doteq O$, für $p_i \neq c_i$ ist $k_i \doteq L$.

Bilden die Chiffrierschritte bezüglich der Zusammensetzung sogar eine kommutative Gruppe, so haben wir die *Kerckhoffs*sche *symétrie de position*

$$\chi_s(t) = \chi_t(s) \ .$$

Für endomorphe Chiffrierungen mit einer kommutativen Schlüsselgruppe ist durch p' und c' der Schlüssel k bereits eindeutig bestimmt:
Mit $c'_i = \chi_{k_i}(p'_i)$ ist auch $c'_i = \chi_{p'_i}(k_i)$ und damit $k_i = \chi^{-1}_{p'_i}(c'_i)$. Die Shannonsche Eigenschaft gilt somit. (Ist also $|M| > N^n$, so ist die Schlüsselgruppe nicht kommutativ. Solche Schlüsselgruppen werden wir in (19.2.4) finden).
Überdies gilt wegen $\chi_{p'_i}(d_i) = p''_i$ auch $\chi_{d_i}(p'_i) = p''_i$. p''_i ergibt sich also aus p'_i durch Chiffrierung mit d_i in der Rolle des Schlüssels.

Zu jeder Schlüsselgruppe gibt es eine Menge **dualer Chiffrierschritte** $\{\breve{\chi}_s\}$,

$$\breve{\chi}_s(p) = s \bullet p^{-1} \ , \quad \breve{\chi}_s^{-1}(c) = c^{-1} \bullet s \quad \text{und} \quad \breve{\chi}_{s \bullet t^{-1}}(p) = \breve{\chi}_{\breve{\chi}_s(t)}(p) \ .$$

Nunmehr gilt $\breve{\chi}^{-1}_{c'_i}(c''_i) = \breve{\chi}_{p''_i}(p'_i)$. Im Falle einer kommutativen Schlüsselgruppe ist die duale Chiffrierung involutorisch: $\breve{\chi}_s^{-1}(t) = \breve{\chi}_s(t)$.

19.2.3 Wenn insbesondere (für $n = 1$) begleitende Alphabete durch eine volle zyklische Verschiebung eines Referenzalphabets von N Zeichen entstehen, so fällt die Anzahl der Schlüssel mit der Anzahl der Zeichen zusammen; es ergibt sich eine Schlüsselgruppe, die kommutativ ist, nämlich die zyklische Gruppe $\mathcal{C}_N$ der Ordnung N. Für VIGENÈRE-Chiffrierschritte trifft dies zu; mit der Addition modulo N als Modell, dual für BEAUFORT-Chiffrierschritte, wie sie in der M-209 von Boris Hagelin gebraucht werden. Hier sind die Referenzalphabete von vornherein bekannt.

ALBERTI-Chiffrierung kann ebenso behandelt werden, wenn die Definition der Differenz geeignet modifiziert wird. So entsteht die von *Kerckhoffs* verwendete Chiffriertabelle (18.5.1, Tabelle 23) durch Verschiebungen ρ^i eines einzigen Chiffrierschritts mit dem Referenzalphabet

P:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	Z	Y	T	V	W	D	F	G	H	J	K	M	Q	N	O	X	R	E	S	P	U	B	L	I	C	A

,
es ist $A = \rho^0 P$, $B = \rho^1 P$, $C = \rho^2 P$, $D = \rho^3 P$, $\ldots$, $Z = \rho^{25} P$.

Daß das permutierte Alphabet P bekannt ist, darf angenommen werden – etwa weil eine *Alberti*-Scheibe in Feindeshand gefallen ist.

Es seien nun die schon in 19.1 untersuchten Geheimtexte (i) und (ii) nochmals betrachtet. Bildet man zu $c'' \stackrel{\text{def}}{=}$ (ii) und $c' \stackrel{\text{def}}{=}$ (i) die P-modifizierte Differenz $d_i = \chi^{-1}_{P^{-1}c'_i}(P^{-1}c''_i)$, so bedeutet $d_i \mathrel{\hat{=}} \rho^{\delta_i} P$, daß man im bekannten permutierten Alphabet P δ_i Schritte weiterzählen muß, um von c''_i zu c'_i zu gelangen. Es ergibt sich

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
c''	U	H	W	P	R	B	Q	L	K	I	B	L	W	R	E	J	R	B	K	L	H	I
c'	U	H	Y	B	R	J	I	M	B	C	F	A	M	M	F	J	H	D	M	R	I	Q
d	a	a	x	c	a	o	l	p	l	b	l	d	h	v	p	a	s	k	b	u	p	p
δ	0	0	23	2	0	14	11	15	11	1	11	3	7	21	15	0	18	10	1	20	15	15

Nunmehr ist $d_i = \chi^{-1}_{P^{-1}c'_i}(P^{-1}c''_i) = \chi^{-1}_{P^{-1}p'_i}(P^{-1}p''_i)$; das bekannte d kann als Geheimtext aufgefaßt werden, der unter χ^{-1} mit $P^{-1}p'$ als (unbekanntem) Schlüssel aus $P^{-1}p''$ als (unbekanntem) Klartext entstanden ist. Durch diesen **Rollenwechsel** sind alle Möglichkeiten des Angriffs mit Häufigkeitsuntersuchungen und Mustererkennungen gegeben.

Beispielsweise bedeutet $d_i = \mathtt{a}$ (das für $i = 1, 2, 5, 16$ auftritt) Übereinstimmung von p'_i und p''_i. Sie wird am häufigsten (im Französischen mit etwa 30%) für $p'_i = p''_i =$ /e/ erfolgen, während $p'_i = p''_i =$ /a/ und $p'_i = p''_i =$ /s/ nur mit je etwa 10% auftreten. (Tatsächlich wäre die kühne Annahme /e/ für $i = 2, 5, 16$ erfüllt, während /l/ für $i = 1$ auftritt.) Die Methode des wahrscheinlichen Worts ist wohl – sofern geeignete Informationen vorliegen – unbedingt angebracht. In unserem Fall kann, den von *Kerckhoffs* geschilderten Umständen zufolge, die französische Sprache angenommen und *ennemi* als wahrscheinliches Wort herangezogen werden. Zu prüfen ist, ob einer möglichen Lage von *ennemi* in p'' ein sinnvolles französisches Wort in p' entspricht (oder umgekehrt). Die folgenden sukzessiven Versuche

	1	2	3	4	5	6	7	8	9
p''	e	n	n	e	m	i	*	*	*
d	a	a	x	c	a	o	l	p	l
δ	0	0	23	2	0	14	11	15	11
p'	e	n	k	g	m	w	*	*	*

	1	2	3	4	5	6	7	8	9
p''	*	*	e	n	n	e	m	i	*
d	a	a	x	c	a	o	l	p	l
δ	0	0	23	2	0	14	11	15	11
p'	*	*	b	p	n	s	x	x	*

	1	2	3	4	5	6	7	8	9
p''	*	e	n	n	e	m	i	*	*
d	a	a	x	c	a	o	l	p	l
δ	0	0	23	2	0	14	11	15	11
p'	*	e	k	p	e	a	t	*	*

	1	2	3	4	5	6	7	8	9
p''	*	*	*	e	n	n	e	m	i
d	a	a	x	c	a	o	l	p	l
δ	0	0	23	2	0	14	11	15	11
p'	*	*	*	g	n	b	p	b	t

führen zunächst zu nichts, erst (und einzig) in der dreizehnten Lage

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
p''	*	*	*	*	*	*	*	*	*	*	*	*	e	n	n	e	m	i	*	*	*	*
d	a	a	x	c	a	o	l	p	l	b	l	d	h	v	p	a	s	k	b	u	p	p
δ	0	0	23	2	0	14	11	15	11	1	11	3	7	21	15	0	18	10	1	20	15	15
p'	*	*	*	*	*	*	*	*	*	*	*	*	l	i	c	e	e	s	*	*	*	*

entsteht mit /licees/ etwas Brauchbares, das vernünftig zu /police est/ fortgesetzt werden kann. (Umgekehrt liefert /ennemi/ in p' nichts Brauchbares.) Vertauscht man jetzt die Rollen von p' und p'', so entsteht

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
p''	*	*	*	*	*	*	*	*	*	*	e	l	e	n	n	e	m	i	s	*	*	*
d	a	a	x	c	a	o	l	p	l	b	l	d	h	v	p	a	s	k	b	u	p	p
δ	0	0	23	2	0	14	11	15	11	1	11	3	7	21	15	0	18	10	1	20	15	15
p'	*	*	*	*	*	*	*	*	*	*	p	o	l	i	c	e	e	s	t	*	*	*

was eine Ergänzung zu /de l' ennemi sont/ nahelegt. Umgekehrt ergibt sich wieder

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
p''	*	*	*	*	*	*	*	*	*	d	e	l	e	n	n	e	m	i	s	o	n	t
d	a	a	x	c	a	o	l	p	l	b	l	d	h	v	p	a	s	k	b	u	p	p
δ	0	0	23	2	0	14	11	15	11	1	11	3	7	21	15	0	18	10	1	20	15	15
p'	*	*	*	*	*	*	*	*	*	e	p	o	l	i	c	e	e	s	t	i	c	i

Auf diese Weise kann ein wahrscheinliches Wort als Keim dienen, von dem ausgehend, nach rechts wie auch nach links, im Zick-Zack (vgl. 14.4.3) der eine und der andere Klartext stückweise verlängert wird. Die Methode erlaubt insbesondere die Heranziehung von Formwörtern, Vorsilben und Endungen, die ja ziemlich häufig vorkommen, etwa /und/, /ein/, /ung/, /bar/, /heit/, /unter/ im Deutschen, /and/, /the/, /that/, /which/, /under/, /tion/ im Englischen, /les/, /que/, /ion/ im Französischen. In unserem Beispiel kann ein neuer Keim weiterführen, mit /les/ ergibt sich aus

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
p''	l	e	s	*	*	*	*	*	*	d	e	l	e	n	n	e	m	i	s	o	n	t
d	a	a	x	c	a	o	l	p	l	b	l	d	h	v	p	a	s	k	b	u	p	p
δ	0	0	23	2	0	14	11	15	11	1	11	3	7	21	15	0	18	10	1	20	15	15
p'	l	e	p	*	*	*	*	*	*	e	p	o	l	i	c	e	e	s	t	i	c	i

mit viel Glück vielleicht die Ergänzung /leprefetd/von p' und damit die Bestätigung durch die Ergänzung /lespertes/ von p'' :

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
p''	l	e	s	p	e	r	t	e	s	d	e	l	e	n	n	e	m	i	s	o	n	t
d	a	a	x	c	a	o	l	p	l	b	l	d	h	v	p	a	s	k	b	u	p	p
δ	0	0	23	2	0	14	11	15	11	1	11	3	7	21	15	0	18	10	1	20	15	15
p'	l	e	p	r	e	f	e	t	d	e	p	o	l	i	c	e	e	s	t	i	c	i

Damit ist die Entzifferung beider Chiffrate gelungen. Selbstverständlich kann nur die Entzifferung des kürzeren zweier solcher Geheimtexte vollständig gelingen. Der Schlüssel wurde dabei überhaupt nicht benützt. Er kann aber jetzt rekonstruiert werden: Die Gegenüberstellung von p' und c' liefert nach der (ohnehin als bekannt vorausgesetzten) Chiffriertabelle wiederum

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
c'	U	H	Y	B	R	J	I	M	B	C	F	A	M	M	F	J	H	D	M	R	I	Q
p'	l	e	p	r	e	f	e	t	d	e	p	o	l	i	c	e	e	s	t	i	c	i
k	*J*	*E*	*M*	*E*	*M*	*E*	*T*	*S*	*S*	*U*	*R*	*L*	*A*	*D*	*E*	*F*	*E*	*N*	*S*	*I*	*V*	*E*

und damit einen ‚verständlichen' Schlüsselsatz. Für den Erfolg dieses **Zick-Zack-Verfahrens** war ausreichend, daß jeder der beiden Klartexte deutlich mehr als 50% Redundanz besitzt.

19.2.4 Die eben behandelte, für ALBERTI-Chiffrierschritte und speziell für VIGENERE-Chiffrierschritte (dual: BEAUFORT-Chiffrierschritte) typische Schlüsselgruppe ist, wie gesagt, die zyklische Gruppe $\mathcal{C}_N$ der Ordnung N für $V = W = \mathbb{Z}_N$. Sie ist nur ein Beispiel für Gruppen vorgeschriebener Ordnung. Für $\mathbb{Z}_{26}$ ist neben der zyklischen Gruppe $\mathcal{C}_{26}$ eine weitere kommutative Gruppe zu nennen: das direkte Produkt $\mathcal{C}_2 \times \mathcal{C}_{13}$ der zyklischen Gruppe der

Ordnung 2 und der zyklischen Gruppe der Ordnung 13. Man stößt auf sie durch eine zwischengeschaltete Codierung $\mathbb{Z}_{26} \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_{13}$. (Eine Menge von k PORTA-Chiffrierschritten (vgl. Abb. 53 für k=11, Abb. 69 für k=10) bildet zwar selbst keine Gruppe, erzeugt jedoch durch Zusammensetzungen $\mathcal{C}_2 \times \mathcal{C}_k$.) Es gibt aber auch eine nichtkommutative Gruppe der Ordnung 26, die Diedergruppe $\mathcal{D}_{13}$, mit den Erzeugenden S und T; $S^{13} = T^2 = (ST)^2 = I$. Sie scheint kryptologisch keine Beachtung gefunden zu haben.

Für $\mathbb{Z}_{25}$ ist neben der zyklischen Gruppe $\mathcal{C}_{25}$ eine weitere kommutative Gruppe das direkte Produkt $\mathcal{C}_5^2 \doteq \mathcal{C}_5 \times \mathcal{C}_5$ zweier zyklischen Gruppen der Ordnung 5, man wird darauf geführt durch die zwischengeschaltete Polybius-Codierung $\mathbb{Z}_{25} \longrightarrow \mathbb{Z}_5 \times \mathbb{Z}_5$. Es gibt keine nichtkommutative Gruppe der Ordnung 25. Für $\mathbb{Z}_{10}$ gibt es neben der zyklischen Gruppe $\mathcal{C}_{10}$ die kommutative Gruppe $\mathcal{C}_2 \times \mathcal{C}_5$; die zwischengeschaltete biquinäre Codierung $\mathbb{Z}_{10} \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_5$ führt zu ihr. Daneben gibt es die nichtkommutative Diedergruppe $\mathcal{D}_5$ mit den Erzeugenden S und T; $S^5 = T^2 = (ST)^2 = I$.

Im Hinblick auf Binärcodierungen besonders interessant sind Gruppen einer Ordnung 2^n. Für beliebiges j gibt es von dieser Ordnung die kommutativen Gruppen $\mathcal{C}_{2^j}$ und $\mathcal{C}_2^j \doteq \mathcal{C}_2 \times \mathcal{C}_2 \times \ldots \times \mathcal{C}_2$. Im schon besprochenen Fall $j = 1$ fallen beide zusammen; für $j = 2$ handelt es sich um die zyklische Vierergruppe einerseits und die *Klein*sche Vierergruppe andrerseits. Für $j = 3$ kommen hinzu die nichtkommutative Quaternionengruppe $\mathcal{Q}$ und die nichtkommutative Diedergruppe $\mathcal{D}_4$ mit den Erzeugenden S und T; $S^4 = T^2 = (ST)^2 = I$, beide ohne kryptologischen Belang. Das gilt auch für eine Fülle nichtkommutativer Gruppen für $j = 4$ und für $j = 5$.

Für den Unterschied zwischen $\mathbb{Z}_{2^n}$ und $\mathbb{Z}_2^n$ (wie auch für den zwischen $\mathbb{Z}_{10^n}$ und $\mathbb{Z}_{10}^n$), nämlich den Fortfall der Übertragseinrichtung, siehe 8.3.3.

0	t	4	o	2	h	n	m	5	l	r	g	i	p	c	v	e	z	d	b	s	y	f	x	a	w	j	3	u	q	k	1	
O	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	1
O	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**O**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	2
O	**O**	**O**	**O**	**L**	**L**	**L**	**L**	**O**	**O**	**O**	**O**	**L**	**L**	**L**	**L**	**O**	**O**	**O**	**O**	**L**	**L**	**L**	**L**	**O**	**O**	**O**	**O**	**L**	**L**	**L**	**L**	3
O	**O**	**L**	**L**	**O**	**O**	**L**	**L**	**O**	**O**	**L**	**L**	**O**	**O**	**L**	**L**	**O**	**O**	**L**	**L**	**O**	**O**	**L**	**L**	**O**	**O**	**L**	**L**	**O**	**O**	**L**	**L**	4
O	**L**	**O**	**L**	**O**	**L**	**O**	**L**	**O**	**L**	**O**	**L**	**O**	**L**	**O**	**L**	**O**	**L**	**O**	**L**	**O**	**L**	**O**	**L**	**O**	**L**	**O**	**L**	**O**	**L**	**O**	**L**	5
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	

Tabelle 24. Binärcodierung des Internationalen Fernschreibalphabets Nr. 2 (CCIT 2)
0: Leer, 1: Buchstaben, 2: Zwischenraum, 3: Ziffern, 4: Wagenrücklauf, 5: Zeilenvorschub

19.2.5 Für $\mathbb{Z}_{2^5}$, den Zeichenvorrat des auf *Donald Murray* (1900) zurückgehenden Internationalen Fernschreibalphabets Nr. 2 (CCIT 2) von 1929 liegt es nahe, eine Chiffrierung (mit $n = 5$) zu verwenden, deren Schlüsselgruppe $\mathcal{C}_2^n$ (und nicht $\mathcal{C}_{2^n}$) ist, nämlich eine Chiffrierung mit 32 Alphabeten, die durch Substitutionen O oder L (8.3.1) der fünf Binärzeichen entstehen. Die Codierung $\mathbb{Z}_{32} \longrightarrow \mathbb{Z}_2^5$ des CCIT 2 zeigt Tabelle 24. Neben den 26 Buchstaben stehen sechs Funktionszeichen des Fernschreibers zur Verfügung, de-

ren Funktion im Chiffrierbetrieb unterbunden wird; wir bezeichnen sie mit 0, 1, 2, 3, 4, 5 und verwenden 2 als Trennzeichen (tatsächlich wurde aus betrieblichen Gründen die Kombination 12 verwendet – dies ergab, s. 19.2.7, eine von *Beurling* genutzte Einbruchmöglichkeit). Werden die Schlüssel durch *0, A, B, C,..., Z, 2, 3, 4, 5, 1* bezeichnet, so zeigt Tabelle 25 die natürliche Chiffriertabelle, ein lateinisches Quadrat.

	0	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	2	3	4	5	1
0	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	2	3	4	5	1
A	A	0	G	F	R	5	C	B	Q	S	4	N	Z	1	K	3	Y	H	D	I	W	2	X	T	V	P	L	U	O	J	E	M
B	B	G	0	Q	T	O	H	A	F	1	L	P	J	S	Y	E	K	C	W	M	D	V	U	R	2	N	4	X	5	Z	3	I
C	C	F	Q	0	U	K	A	H	G	4	S	E	M	L	5	P	O	B	2	J	V	D	T	X	W	3	1	R	Y	I	N	Z
D	D	R	T	U	0	4	2	W	X	K	5	I	3	Y	S	Z	1	V	A	N	B	C	Q	G	H	M	O	F	L	E	J	P
E	E	5	O	K	4	0	N	3	Y	U	R	C	W	X	F	B	Q	P	J	2	Z	I	1	L	M	H	T	S	G	D	A	V
F	F	C	H	A	2	N	0	Q	B	J	I	5	1	Z	E	Y	3	G	U	4	X	R	W	V	T	O	M	D	P	S	K	L
G	G	B	A	H	W	3	Q	0	C	M	Z	Y	4	I	P	5	N	F	T	1	R	X	2	D	U	K	J	V	E	L	O	S
H	H	Q	F	G	X	Y	B	C	0	L	1	3	I	4	O	N	5	A	V	Z	2	W	R	U	D	E	S	T	K	M	P	J
I	I	S	1	4	K	U	J	M	L	0	F	D	H	G	R	V	T	Z	N	A	P	E	O	Y	3	W	Q	5	X	C	2	B
J	J	4	L	S	5	R	I	Z	1	F	0	2	B	Q	U	W	X	M	E	C	3	N	Y	O	P	V	G	K	T	A	D	H
K	K	N	P	E	I	C	5	Y	3	D	2	0	X	W	A	Q	B	O	S	R	1	4	Z	M	L	G	V	J	H	U	F	T
L	L	Z	J	M	3	W	1	4	I	H	B	X	0	C	V	R	2	S	O	Q	5	Y	N	E	K	U	A	P	D	G	T	F
M	M	1	S	L	Y	X	Z	I	4	G	Q	W	C	0	T	2	R	J	P	B	N	3	5	K	E	D	F	O	U	H	V	A
N	N	K	Y	5	S	F	E	P	O	R	U	A	V	T	0	H	G	3	I	D	M	J	L	1	Z	B	X	4	Q	2	C	W
O	O	3	E	P	Z	B	Y	5	N	V	W	Q	R	2	H	0	C	K	L	X	4	1	I	J	S	F	D	M	A	T	G	U
P	P	Y	K	O	1	Q	3	N	5	T	X	B	2	R	G	C	0	E	M	W	I	Z	4	S	J	A	U	L	F	V	H	D
Q	Q	H	C	B	V	P	G	F	A	Z	M	O	S	J	3	K	E	0	X	L	U	T	D	2	R	5	I	W	N	1	Y	4
R	R	D	W	2	A	J	U	T	V	N	E	S	O	P	I	L	M	X	0	K	G	F	H	B	Q	1	3	C	Z	5	4	Y
S	S	I	M	J	N	2	4	1	Z	A	C	R	Q	B	D	X	W	L	K	0	Y	5	3	P	O	T	H	E	V	F	U	G
T	T	W	D	V	B	Z	X	R	2	P	3	1	5	N	M	4	I	U	G	Y	0	Q	C	A	F	S	E	H	J	O	L	K
U	U	2	V	D	C	I	R	X	W	E	N	4	Y	3	J	1	Z	T	F	5	Q	0	B	H	G	L	P	A	M	K	S	O
V	V	X	U	T	Q	1	W	2	R	O	Y	Z	N	5	L	I	4	D	H	3	C	B	0	F	A	J	K	G	S	P	M	E
W	W	T	R	X	G	L	V	D	U	Y	O	M	E	K	1	J	S	2	B	P	A	H	F	0	C	I	5	Q	4	3	Z	N
X	X	V	2	W	H	M	T	U	D	3	P	L	K	E	Z	S	J	R	Q	O	F	G	A	C	0	4	N	B	I	Y	1	5
Y	Y	P	N	3	M	H	O	K	E	W	V	G	U	D	B	F	A	5	1	T	S	L	J	I	4	0	2	Z	C	X	Q	R
Z	Z	L	4	1	O	T	M	J	S	Q	G	V	A	F	X	D	U	I	3	H	E	P	K	5	N	2	0	Y	R	B	W	C
2	2	U	X	R	F	S	D	V	T	5	K	J	P	O	4	M	L	W	C	E	H	A	G	Q	B	Z	Y	0	1	N	I	3
3	3	O	5	Y	L	G	P	E	K	X	T	H	D	U	Q	A	F	N	Z	V	J	M	S	4	I	C	R	1	0	W	B	2
4	4	J	Z	I	E	D	S	L	M	C	A	U	G	H	2	T	V	1	5	F	O	K	P	3	Y	X	B	N	W	0	R	Q
5	5	E	3	N	J	A	K	O	P	2	D	F	T	V	C	G	H	Y	4	U	L	S	M	Z	1	Q	W	I	B	R	0	X
1	1	M	I	Z	P	V	L	S	J	B	H	T	F	A	W	U	D	4	Y	G	K	O	E	N	5	R	C	3	2	Q	X	0

Tabelle 25. Chiffriertabelle für Fernschreibzeichen: Addition modulo 2 in $\mathbb{Z}_2^5$

Die Fernschreibcodierung war seit der Jahrhundertwende weithin bekannt und seit *Vernam* auch den professionellen Kryptologen geläufig; die naheliegende Schlüsselgruppe $\mathcal{C}_2^n$ und damit die Chiffriertabelle war konkret bekannt. Es lagen also alle Voraussetzungen für einen Angriff nach 19.2.3 vor, insbesondere war (nach 19.2.2 wegen der Kommutativität der Schlüsselgruppe zwangsläufig) der Schlüssel aus Geheimtext und Klartext rekonstruierbar.

Ein fiktives Beispiel mag sich nun so abgespielt haben: Zwei ungefähr gleichlange Funksprüche zur Zeit des deutschen Angriffs auf Kreta (Mitte Mai 1941) enthielten nach übereinstimmenden Präambeln die (vermutlich phasengleichen) Textanfänge (im Jargon von Bletchley Park eine 'depth of two')

2 W H N R	G 1 A T U	A P L B V	R W O U F	Y P B S X	Z N R 4 J	S R
L 0 G 2 A	W G H 2 Z	K B V Z V	Q Z W Y K	Y W J I 0	K T 5 A Z	2 K

Die Briten bildeten die Differenz

	1 2 3 4 5	6 7 8 9 10	11 12 13 14 15	16 17 18 19 20	21 22 23 24 25	26 27 28 29 30	31 32
c''	2 W H N R	G 1 A T U	A P L B V	R W O U F	Y P B S X	Z N R 4 J	S R
c'	L 0 G 2 A	W G H 2 Z	K B V Z V	Q Z W Y K	Y W J I 0	K T 5 A Z	2 K
d	f w c w d	d v q k p	n k n 4 0	x 5 j l 5	0 s l a x	v m 4 j g	g s

und suchten mit dem wahrscheinlichen Wort /2kreta2/ ein verständliches Gegenstück, wurden schließlich auch fündig mit

	1 2 3 4 5	6 7 8 9 10	11 12 13 14 15	16 17 18 19 20	21 22 23 24 25	26 27 28 29 30	31 32
p''	* * * 2 k	r e t a 2	* * * * *	* * * * *	* * * * *	* * * * *	* *
d	f w c w d	d v q k p	n k n 4 0	x 5 j l 5	0 s l a x	v m 4 j g	g s
p'	* * * n i	a 2 u n d	* * * * *	* * * * *	* * * * *	* * * * *	* *

Ein Blick auf die Landkarte legt eine Ergänzung von p'' zu /chania/ nahe und liefert:

	1 2 3 4 5	6 7 8 9 10	11 12 13 14 15	16 17 18 19 20	21 22 23 24 25	26 27 28 29 30	31 32
p''	a u f 2 k	r e t a 2	* * * * *	* * * * *	* * * * *	* * * * *	* *
d	f w c w d	d v q k p	n k n 4 0	x 5 j l 5	0 s l a x	v m 4 j g	g s
p'	c h a n i	a 2 u n d	* * * * *	* * * * *	* * * * *	* * * * *	* *

Nunmehr konnten sie einige andere Ortsnamen probieren, die dem /und/ folgen. Ein anderer Weg ist, ein weiteres wahrscheinliches Wort zu versuchen, etwa /2angriff2/. Damit wurden die Briten bei p'' in der Lage 19 fündig mit

	1 2 3 4 5	6 7 8 9 10	11 12 13 14 15	16 17 18 19 20	21 22 23 24 25	26 27 28 29 30	31 32
p''	a u f 2 k	r e t a 2	* * * * *	* * * 2 a	n g r i f	f 2 * * *	* *
d	f w c w d	d v q k p	n k n 4 0	x 5 j l 5	0 s l a x	v m 4 j g	g s
p'	c h a n i	a 2 u n d	* * * * *	* * * f e	n 2 o s t	w a e * *	* *

Nun geht es schon fast im Galopp weiter; das fehlende Stück in p' dürfte /2die2haefen/ sein, anschließend steht vermutlich /ostwaerts2/. Das ergibt

	1 2 3 4 5	6 7 8 9 10	11 12 13 14 15	16 17 18 19 20	21 22 23 24 25	26 27 28 29 30	31 32
p''	a u f 2 k	r e t a 2	w i r d 2	d e r 2 a	n g r i f	f 2 d e r	2 g
d	f w c w d	d v q k p	n k n 4 0	x 5 j l 5	0 s l a x	v m 4 j g	g s
p'	c h a n i	a 2 u n d	2 d i e 2	h a e f e	n 2 o s t	w a e r t	s 2

In besser lesbarer Form

auf_kreta_wird_der_angriff_der_g .....   *chania_und_die_haefen_ostwaerts_* .....

Ganz ähnlich konnte man mit anderen Teilen des Textes verfahren. Eine solche Arbeit war mühevoll, aber sicher auch reizvoll.

Nach vollendeter Dechiffrierung konnte nun auch der Schlüssel rekonstruiert werden. Da aber in $\mathcal{C}_2^n$ die Subtraktion mit der Addition zusammenfällt, war herauszufinden, welcher Geheimtext zu welchem Klartext gehörte. Die beiden möglichen Zuordnungen ergeben

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
p'	c	h	a	n	i	a	2	u	n	d	2	d	i	e	2	h	a	e	f	e	n	2	o	s	t	w	a	e	r	t	s	2
k_1	*M*	*H*	*B*	*W*	*S*	*T*	*S*	*W*	*W*	*O*	*T*	*T*	*O*	*T*	*E*	*A*	*L*	*L*	*O*	*C*	*B*	*N*	*W*	*A*	*T*	*M*	*W*	*A*	*D*	*E*	*G*	*T*
c'	L	0	G	2	A	W	G	H	2	Z	K	B	V	Z	V	Q	Z	W	Y	K	Y	W	J	I	0	K	T	5	A	Z	2	K

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
p''	a	u	f	2	k	r	e	t	a	2	w	i	r	d	2	d	e	r	2	a	n	g	r	i	f	f	2	d	e	r	2	g
k_2	*Z*	*U*	*Q*	*0*	*N*	*B*	*3*	*6*	*M*	*C*	*M*	*2*	*H*	*O*	*E*	*V*	*T*	*B*	*R*	*N*	*B*	*D*	*E*	*0*	*F*	*5*	*K*	*J*	*5*	*3*	*0*	*Y*
c'	L	0	G	2	A	W	G	H	2	Z	K	B	V	Z	V	Q	Z	W	Y	K	Y	W	J	I	0	K	T	5	A	Z	2	K

Man wird sich vielleicht für eine weniger unregelmäßige, wie hier die erstere, Lösung entschieden haben, in der Annahme, daß durch einen nicht zu komplizierten Schlüsselerzeuger eine gewisse (lokale) Regelmäßigkeit unvermeidbar sein dürfte.

19.2.6 Die Verwendung des Chiffrierfernschreibers SZ40, SZ42 („Schlüsselzusatz“) der Firma Lorenz, in dem eine Schlüsselfolge durch ‚unregelmäßige‘ Fortschaltung erzeugt wurde, auf der höchsten Ebene der Wehrmacht-Nachrichtenverbindungen war also äußerst riskant, wenn man eine Klartext-Klartext-Kompromittierung nicht ausschließen konnte. *P. W. Filby* berichtete überdies, daß 1932 ein *Mr. Lorenz* dem *Foreign Office* eine Chiffriermaschine angeboten und offenbart hatte. Hinzu kam, daß das Konkurrenzprodukt der Firma Siemens, der Chiffrierfernschreiber T52 („Geheimschreiber“), offen beschrieben war im DRP Nr. 615016, angemeldet von *August Jipp* und *Ehrhard Roßberg* am 18. Juli 1930, U.S. Patent No. 1 912 983 für *Jipp*, *Rossberg*, und *Eberhard Hettler*. Es war also für die Briten in *Bletchley Park* nicht allzu schwer, die Situation richtig zu beurteilen. Zugute kam ihnen, daß der „Schlüsselzusatz“ tatsächlich nur die 32 durch Substitutionen O oder L der fünf Binärzeichen entstehenden Chiffrierschritte benutzte, während der T52 auch Transpositionen heranzog (9.1.3) und eine größere Schlüsselmenge hatte.


John H. Tiltman

Die für die deutsche Seite fatale Situation trat tatsächlich ein, und zwar sehr früh. Wie man seit 1993 durch *Jack Good* (erste Andeutungen 1978 durch *Brian Johnson*, 1983 durch *Andrew Hodges*) weiß, wurden auf der seit Mitte 1941 bestehenden Hellschreiber-Funkstrecke Wien–Athen der Wehrmacht noch während der Erprobung infolge eines Fehlers eines deutschen Nachrichtensoldaten zwei ziemlich lange Nachrichten p', p'' mit der selben Anfangsstellung der ‚Schlüsselräder‘ ausgesandt, also mit dem selben Schlüssel k chiffriert. Irgend jemand in *Bletchley Park* schöpfte Verdacht; die Kompromittierung erlaubte dem Oberst, später Brigadegeneral *John Tiltman*,[2] dem Chef des britischen Dechiffrierwesens in *Bletchley Park*, im Herbst 1941 aus der Differenz d der beiden aufgefangenen Geheimtexte in zweiwöchiger Handarbeit die beiden Klartexte zu bestimmen.

[2] “... he was charming and intelligent and though he looked military he certainly didn’t behave like a stuffed shirt.” (*Robin Denniston*)

Wie zwischenzeitlich bekannt wurde, fand der Vorfall am 30. August 1941 statt; mit dem Indikator HQIBPEXEZMUG wurden zwei ungefähr 4000 Zeichen umfassende vermutliche *isologs* aufgefangen, die in den ersten 7 Zeichen übereinstimmten und deren Zeichen #51 bis #120 nachfolgend zusammen mit der Differenzenbildung, die *Tiltman* vornahm, wiedergegeben sind:

	51 52 53 54 55	56 57 58 59 60	61 62 63 64 65	66 67 68 69 70	71 72 73 74 75	76 77 78 79 80	81 82 83 84 85
c''	U B 2 3 R	5 W E V G	Q I 2 4 5	G R J M L	C Y 5 0 H	K A S 1 I	S 5 X U N
c'	Y U H V H	3 H E E 0	T G 2 H H	1 Q J X V	K 1 B J M	K 2 O M Z	Y V I N 3
d	l v t s v	b u 0 1 g	u m 0 m p	s x 0 e n	e r 3 j 4	0 u x a q	t m 3 j q

	86 87 88 89 90	91 92 93 94 95	96 97 98 99 00	01 02 03 04 05	06 07 08 09 10	11 12 13 14 15	16 17 18 19 20
c''	S R Z Z B	D B B 1 C	L S Q H H	U H 5 X D	0 F N 3 J	3 V O C A	D J C D N
c'	H M C 3 D	U Q 3 4 Z	R 2 M R M	O H * J Q	P W U E Y	C D R G 1	L D A T I
d	z p 1 r t	c c 5 q 1	o e j v 4	1 0 * p v	p v j g v	y q l h m	3 5 f b r

Tiltman mag vielleicht mit dem wahrscheinlichen Wort /geheim2/ ein verständliches Gegenstück gesucht haben, dabei wurde er sicher bald fündig mit

	61 62 63 64 65	66 67 68 69 70	71 72 73 74 75	76 77 78 79 80	81 82 83 84 85	86 87 88 89 90	91 92 93 94 95
p''	* * * * g	e h e i m	2 * * * *	* * * * *	* * g e h	e i m 2 *	* * * * *
d	u m 0 m p	s x 0 e n	e r e j 4	0 u x a q	t m 3 j q	z p 1 r t	c c 5 q 1
p'	* * * * n	2 d e u t	s * * * *	* * * * *	* * e r a	t t a c *	* * * * *

/n2deuts/ läßt sich unschwer zu /an2deutsch/ ergänzen, ebenso führt /erattac/ auf /2militaerattache2/ ; die Lücke füllt sich mit /an2deutschen/ . Das ergibt für p' bereits ein Fragment von 29 Zeichen:

	61 62 63 64 65	66 67 68 69 70	71 72 73 74 75	76 77 78 79 80	81 82 83 84 85	86 87 88 89 90	91 92 93 94 95
p''	* * * * g	e h e i m	2 * * * *	* * * * *	* * g e h	e i m 2 *	* * * * *
d	u m 0 m p	s x 0 e n	e r e j 4	0 u x a q	t m 3 j q	z p 1 r t	c c 5 q 1
p'	* * * a n	2 d e u t	s c h e n	2 m i l i	t a e r a	t t a c h	e 2 * * *

und ergibt für p'' ebenfalls 29 konsekutive Zeichen

	61 62 63 64 65	66 67 68 69 70	71 72 73 74 75	76 77 78 79 80	81 82 83 84 85	86 87 88 89 90	91 92 93 94 95
p''	* * * 1 g	e h e i m	2 2 k r 2	2 3 3 z z	0 1 g e h	e i m 2 2	k r * * *
d	u m 0 m p	s x 0 e n	e r e j 4	0 u x a q	t m 3 j q	z p 1 r t	c c 5 q 1
p'	* * * a n	2 d e u t	s c h e n	2 m i l i	t a e r a	t t a c h	e 2 * * *

Damit ist auch klar, daß, einer liebgewordenen deutschen Gewohnheit folgend, GEHEIM verdoppelt wurde; die Verdopplung der gesamten Gruppe /1geheim22kr2233zz0/ führt auf eine Verlängerung, die bis auf einen Hörfehler Sinn macht. Spätestens jetzt drängt sich der Verdacht auf, daß die weitere Nachricht p'' gegenüber p' lediglich verschoben ist, und zwar um 39 Stellen, weil /an2deutschen2militaerattache2/ in der Lage #103 wieder Sinn ergibt, nämlich /lage11nr33mwoou211g/ (in verständlichem Text *lage nr.2997_g*):

	86 87 88 89 90	91 92 93 94 95	96 97 98 99 00	01 02 03 04 05	06 07 08 09 10	11 12 13 14 15	16 17 18 19 20
p''	e i m 2 2	k r 2 2 3	3 z z 1 2	* * a n 2	d e u t s	c h e n 2	m i l i t
d	z p 1 r t	c c 5 q 1	o e j v 4	1 0 * p v	p v j g v	y q l h m	3 5 f b r
p'	t t a c h	e 2 i w 2	a t h e n	* l a g e	1 1 n r 3	3 m w o o	u 2 1 1 g

Somit ergibt sich nun die weitere Fortsetzung durch Vorausschau um 39 Zeichen bereits automatisch — ganz ähnlich zu dem Trugschluß über *autokey*, den *Shannon* beschrieb (8.7.2). Es wird berichtet, daß *Tiltman* nach zehn Tagen die Entzifferung geschafft hatte, die wegen möglicher weiterer Hörfehler vermutlich schwieriger war, als die nachträgliche Analyse erkennen läßt.

Daß die Chiffrierung tatsächlich durch Addition modulo 2 erfolgte, die Subtraktion also mit der Addition zusammenfiel, hatte übrigens für die Methode keine Bedeutung. Die Chiffrierung war jedoch involutorisch, was die Praxis für vorteilhaft hielt – ohne echt involutorisch, mit den damit verbundenen Nachteilen, zu sein.

Die Nachrichten mögen für sich von geringem Wert gewesen sein. Wichtig war, daß ein rund 4000 Zeichen langes Fragment des von der unbekannten Maschine, britischer Deckname TUNNY (Thunfisch) erzeugten Schlüssels exponiert war, nämlich durch $k = c' + p' \bmod 2$; der Anfang lautete (Tab. 24):

	61 62 63 64 65	66 67 68 69 70	71 72 73 74 75	76 77 78 79 80	81 82 83 84 85	86 87 88 89 90
k	∗ ∗ ∗ *Q O*	*3 V R G C*	*R Z F R T*	*J O V C Q*	*S X U I O*	*2 N F Y X*
1	**L O**	**L O O O O**	**O L L O O**	**L O O O L**	**L L L O O**	**O O L L L**
2	**L O**	**L L L L L**	**L O O L O**	**L O L L L**	**O O L L O**	**O O O O O**
3	**L O**	**O L O O L**	**O O L O O**	**O O L L L**	**L L L L O**	**L L L L L**
4	**O O**	**L L L L L**	**L O L L O**	**L L L L O**	**O L O O L**	**O L L O L**
5	**L L**	**L L O L O**	**O L O O L**	**O L L O L**	**O L O O L**	**O O O L L**

	91 92 93 94 95	96 97 98 99 00	01 02 03 04 05	06 07 08 09 10	11 12 13 14 15	16 17 18 19 20
k	*I W X 2 Y*	∗ *H 4 J T*	∗ *I* ∗ *Z P*	*D N J I C*	*Y R B 5 U*	*Y F M K M*
1	**O L L O L**	**O O L O**	**O** **L O**	**L O L L O**	**L O L O L**	**L L O L O**
2	**L L O O O**	**O O L O**	**L** **O L**	**O O L L L**	**O L O L L**	**O O O L O**
3	**L O L L L**	**L O O O**	**L** **O L**	**O L O O L**	**L O O O L**	**L L L L L**
4	**O O L O O**	**O L L O**	**O** **O O**	**L L L L L**	**O L L O O**	**O L L L L**
5	**O L L O L**	**L O O L**	**O** **L L**	**O O O O O**	**L O L O O**	**L O L O L**

Mit dem Schlüsselfragment der hypothetischen TUNNY-Maschine war ein Einbruch in das Schlüsselerzeugungssystem der deutschen Maschine möglich. Zunächst war es erforderlich, die Perioden die einzelnen Schlüsselräder (auf deren Vorkommen man wohl in Analogie zur Siemens T52 schließen konnte) herauszufinden. Aus der Länge des Indikators konnte man vage schließen, daß 12 Schlüsselräder mitspielten. Da keiner der Kanäle k_1 bis k_5 des Schlüssels k Perioden mit Längen unter 100 aufwies, mußte man annehmen, daß jeder Kanal durch die Wirkung (wenigstens) zweier Schlüsselräder chiffriert wurde. Die Briten nannten sie χ_i und ψ_i, wobei zuerst die *Chi*-Räder und dann die *Psi*-Räder chiffrierten. Durch Parallelstellenuntersuchung fanden sie zuerst die Perioden der *Chi*-Schlüsselräder heraus, etwa 41 für χ_1 , wie Abb. 142 zeigt. Dann wurden auch die Perioden der *Psi*-Schlüsselräder bestimmt (43 für ψ_1) und die Wirkungsweise der verbleibenden zwei *motor wheels* aufgeklärt (s. 9.1.4). Diese Aufgabe löste nach *Johnson* und *Good* in monatelanger Arbeit hauptsächlich der junge Mathematiker *William Tho-*

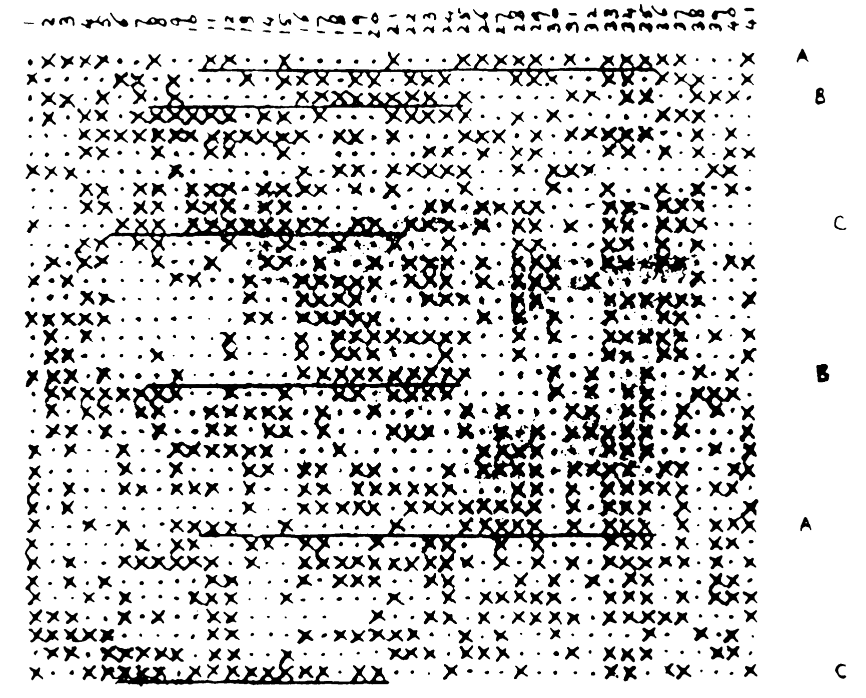


Abb. 142. Periodenbestimmung des Schlüsselrads χ_1. Parallelstellen A, B, C.
In Bletchley Park wurde **O** durch einen Punkt, **L** durch ein Kreuz dargestellt

mas Tutte aus dem Trinity College von Cambridge, der später als Graphentheoretiker bekannt wurde. Die Briten nannten im weiteren Verlauf die Feststellung der durch die Lage der Schaltstifte auf den Schlüsselrädern bestimmten, in kurzen Zeitabständen wechselnden periodischen **O**-**L**-Folgen '*wheel breaking*'. Januar 1942 war die gesamte Struktur der durch das selbe HQIBPEXEZMUG (liebevoll 'ZMUG' genannt) kompromittierten Maschine aufgeklärt; nach Kriegsende bestätigten erbeutete Maschinen dies.[3] Die praktische Arbeit bestand nach dem gelegentlichen '*wheel breaking*' „nur" noch darin, jeweils die richtige Anfangsstellung der Schlüsselräder zu finden ('*wheel setting*') – etwa durch Exhaustion mit vorgegebenen '*cribs*', geeigneten Mengen wahrscheinlicher Wörter; dann lieferte aber die von *S. W. Broadhurst* nachgebaute TUNNY-Maschine (fertig Mitte 1942) den Klartext.

Nach den Anweisungen des von der *pure cryptanalysis* überzeugten *Maxwell H. A. Newman* ging man an die Mechanisierung des '*wheel setting*'. Der aufgefangene Geheimtext mußte gegen den Schlüsseltext phasenrichtig ausgerichtet werden, möglicherweise durch einen Kappa-Test. Mai 1943 war bereits ein erstes Versuchsmodell, nämlich der schon in 17.3.3 genannte HEATH ROBINSON, in Betrieb; wobei auch der ständig umlaufende Schlüssel auf Lochstreifen gestanzt war. Das führte zu Problemen der mechanischen Ab-

[3] "*We did not capture a German TUNNY until the last days of the war in Europe*", sagte stolz *Jack Good.*

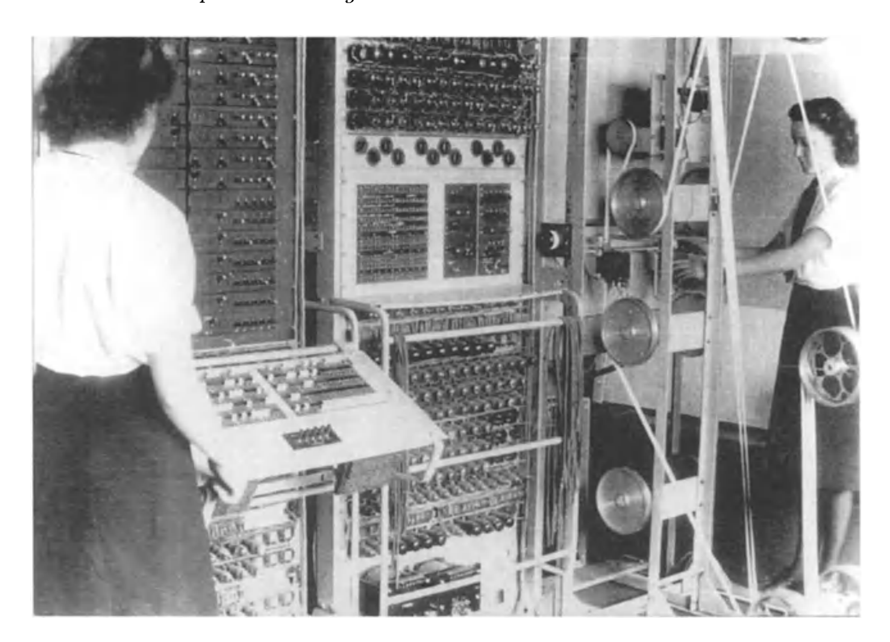


Abb. 143. Teilansicht der COLOSSUS (vermutlich Mark II). Deutlich zu sehen sind der umlaufende Lochstreifen für den Geheimtext, das Klinkensteckerfeld und die Anordnung der Röhren, vermutlich vom Typ *Mullard EF36*

nutzung. *T. H. Flowers* († 1998), unterstützt von *S. W. Broadhurst*, *W. W. Chandler* und von *A. W. M. Coombs*, ging deshalb daran, den Schlüssel intern zu speichern: Im Dezember 1943 wurde der Prototyp COLOSSUS Mark I, weltweit die erste funktionsfähige elektronische Rechenmaschine[4], fertig; ab Februar 1944 wurde sie erfolgreich gegen TUNNY (SZ 42) eingesetzt und am 1. Juni 1944, gerade rechtzeitig zum Beginn der Landung in der Normandie, wurde die verbesserte COLOSSUS Mark II nutzbar (Abb. 143).

In der Anwendung gegen die deutschen Fernschreib-Chiffriermaschinen wurden nach *Johnson* deren Schlüsselräder durch schnelle Röhren-Ringzähler[5] im 1-aus-n-Code nachgebildet. Der Geheimtext-Lochstreifen konnte photoelektrisch mit 5 000 Zeichen pro Sekunde abgelesen werden. COLOSSUS mit ungefähr 1 500 Röhren erlaubte auch eine flexible Klinkenstecker-Programmierung elementarer Boolescher Operationen und binärer (bi-quinärer) Arithmetik, und zwar in fünffacher Parallelisierung. In der verbesserten Mark II mit etwa 2 500 Röhren konnten auch Ablaufverzweigungen bewältigt werden, es gab zudem ein *'logic switching panel'*, ein Schalterfeld, auf dem Boolesche Operationen zwischen den Spuren manuell voreingestellt und während des Ablaufs verändert werden konnten. Nach *Good* wurden die späteren Maschinen auch zur Unterstützung des *wheel breaking* der Chi-Schlüsselräder eingesetzt. Insgesamt wurden zehn COLOSSUS-Maschinen gebaut.

[4] nach *Michie* wohl auch SUPER ROBINSON genannt.

[5] *Johnson*, der aufgrund einer Desinformation unter der irrigen Annahme stand, das Gerät sei gegen den ‚Geheimschreiber' T52 gerichtet gewesen, spricht noch von 10 Zählern.

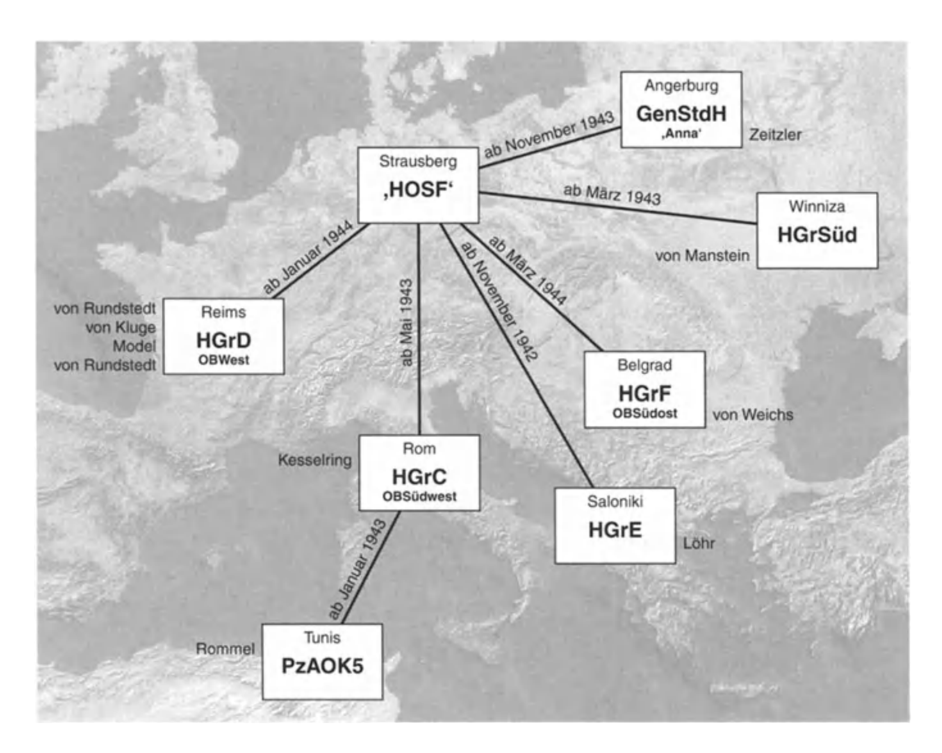


Abb. 144. Einige Funkfernschreibverbindungen mit SZ 40, SZ 42, die in Bletchley Park mit COLOSSUS gebrochen wurden (nach *Hinsley*)

Es schmälert den Ruhm der Briten nicht, wenn man feststellt, daß diese Maschinen hauptsächlich auf ziemlich primitive Vergleichsoperationen getrimmt waren, auf Rechnen im weitesten Sinn. Ihr Steuerungsablauf war auf der gleichen Ebene wie der der Maschinen von *Konrad Zuse*, sie benutzten das Sägebockprinzip. Nach *Good* programmierte *Donald Michie* sie auch, um das '*wheel breaking*' zu beschleunigen. Es ist aber nicht klar, ob die Geräte *auch* für andere Aufgaben als das '*wheel setting*' eingesetzt wurden – zur Periodenanalyse, zum Ausrichten der Phase, zum Abstreifen einer Überchiffrierung, wozu sie (vgl. 17.3.5 und 18.6.3) durchaus geeignet gewesen wären.

In den U.S.A. gab es aufgrund einer Reihe von Fehlschlägen, die *Vannevar Bush* in seinen Versuchen, eine elektronische Version seines COMPARATORs zu bauen, erlitt, vor dem Ende des 2. Weltkriegs keine erfolgreiche elektronische Entwicklung, die den britischen COLOSSUS-Geräten ebenbürtig war. Dann holte die amerikanische Kryptanalyse jedoch auf: "*by the time Japan surrendered, the Americans were building electronic machines using twice as many tubes as the British Colossus*" (*Burke*) – gemeint ist die Eastman 5202.

Die Briten waren ab 1943 gegen die deutschen Funkfernschreibverbindungen der Heeresführung, die überwiegend mit SZ40 und SZ42 arbeiteten, sehr erfolgreich und ergänzten damit ihre hauptsächlich von der Luftwaffe gespeisten ENIGMA-Einbrüche, obschon manchmal, den höheren kryptologischen

Ansprüchen entsprechend, die Entzifferung bedeutend mehr Zeit in Anspruch nahm (normalerweise vier Tage). Die Nachrichten auf höchster Ebene waren den Aufwand wert. Gebrochen wurden ab November 1942 die Verbindung zwischen Berlin und der Heeresgruppe E in Saloniki, ab Januar 1943 die Verbindung zwischen der Heeresgruppe C in Rom und der Panzerarmee von *Rommel* in Tunis. Ab Mai 1943 war die Verbindung zwischen Berlin und der Heeresgruppe C (*Kesselring*) nicht mehr sicher, ab April 1943 auch die Verbindung zwischen Berlin und der Heeresgruppe Süd in Winniza. Die deutsche Offensive gegen Kursk, Juli 1943, wurde damit kompromittiert. An diese frühen Erfolge reihten sich 1944 zahlreiche weitere an, darunter auch der Einbruch in die Verbindung zwischen Berlin und dem Oberkommandierenden der Westfront, *von Rundstedt* (Abb. 144). Die Betroffenen waren ahnungslos. Sie wechselten die *Chi*-Schlüsselräder alle 3 Monate, die *Psi*-Schlüsselräder alle 6 Monate, später alle Monate; die *motor wheels* wurden täglich gewechselt.

Die Briten hatten auch Rückschläge hinzunehmen. Am 10. Juni 1944, vier Tage nach der Landung in der Normandie und zehn Tage nach Inbetriebnahme von COLOSSUS Mark II, verloren sie den Einblick in die Verbindung von Berlin zu *von Rundstedt*, und im Juli auch in die Verbindung von Berlin zu *Kesselring*; erst im September hatten sie wieder aufgeschlossen. Dies beruhte auf einem radikalen Zusatz zur Lorenz-Maschine, ähnlich zu der 'Klartextfunktion' der Siemens-Maschine: Die Briten nannten sie kurz und bündig 'Plaintext Bit 5 Two Steps Back'.

Nunmehr kam auch eine wachsende Zahl von COLOSSUS-Maschinen zum Einsatz. Die britische Entzifferung erreichte einen Höhepunkt im März 1945; von da an reichte die Kraft der zusammenbrechenden Wehrmacht nicht einmal mehr aus, die britischen Entzifferer voll zu beschäftigen. Immerhin kamen die wachsenden Erfolge gegen die SZ42 gerade recht, um die zusehende Erschwerung der Entzifferung der ENIGMA zu kompensieren.

19.2.7 Gegen die Schlüsselfernschreibmaschine T52 von Siemens („Geheimschreiber“) richteten sich die britischen Anstrengungen weniger.[6] Das lag nicht so sehr daran, daß sie tatsächlich, weil ihre Chiffrierschritte auch gewisse Transpositionen der Bits (siehe 9.1.3) einschlossen, kryptologisch umfangreicher und kryptanalytisch etwas widerspenstiger war — T52-chiffrierte Funksprüche wurden, dank sorgloser Operateure auf deutscher Seite, ab Mitte 1942, wenn auch mühevoll, ebenfalls entziffert, erstmals auf den Funkstrecken Sizilien-Libyen und Ägäis-Sizilien —, sondern weil sie aus technischen Gründen auf Funkstrecken nur ungern eingesetzt wurde. Ein weiterer Grund war, daß die Luftwaffe mit ihren ENIGMA-Verbindungen so fahrlässig umging, daß man sich die Mühe mit den von der Luftwaffe benutzten T52 sparen konnte. Umgekehrt war der Einbruch in die ENIGMA-Verbindungen des disziplinierten und weniger geschwätzigen Heeres schwieriger (19.7).

6 Daß COLOSSUS hauptsächlich gegen SZ42 und nicht gegen T52 gerichtet war, wurde erstmals 1980 von *Rex Malik* aufgedeckt.

Die T52a wie auch die aufgerüstete T52d benutzten (s. 9.1.3) neben 32 Substitionen auch 32 Transpositionen der fünf Bits, von denen 30 verschieden waren. Der Schaltungsaufbau dieser Transpositionen war bekannt. Die gegen die SZ42 gerichtete Angriffsmethode konnte *cum grano salis* übertragen werden; die Rekonstruktion des Schlüssels war allerdings komplizierter. Das Bauprinzip der Schlüsselräder war ebenfalls bereits bekannt. Die T52c wie auch die aufgerüstete T52e, die Spruchschlüsseleinstellung hatten, verwendeten nur 16 verschiedene Transpositionen. Und die Aufrüstung zur T52d bzw. T52e war nicht gravierend: Die ‚unregelmäßige' Fortschaltung war kein bedeutendes Hindernis. Sprüche mit Klartextfunktion waren zwar sehr schwierig zu brechen, kamen andrerseits aus technischen Gründen im Funkverkehr nur selten vor.

Superimposition von Sprüchen vom 25. und 27. Mai 1940 erlaubte dem für *Försvarets Radioanstalt* (FRA) arbeitenden schwedischen Mathematiker *Arne Beurling* (1905–1986), ein Genie wie Turing, in eine über Schweden nach Oslo laufende T52a-Fernschreibverbindung einzudringen. Er nützte die betrieblich gebotene stereotype und häufige Verwendung des Fernschreibzeichens 1 'Buchstabenumschaltung' vor jedem 2 'Zwischenraum' (s. 19.2.5) aus: Er beobachtete, daß nicht nur die Klartextzeichen 1 und 2 genau *ein* Bit gemeinsam haben, sondern daß dies auch der Fall ist, wenn sie bei einer der häufig vorkommenden Klartext-Klartext-Kompromittierungen an der selben Schlüsselposition chiffriert werden ('differential cryptanalysis'). Damit konnte er bereits die Wortzwischenräume rekonstruieren. Details, wie er weiter verfuhr, hat er mit ins Grab genommen. Jedenfalls gelang ihm um den 12. Juni 1940 der Einbruch und sodann eine vollständige Rekonstruktion der T52a/b und der Nachbau. Ende 1942 waren 32 der "apps" (Abb. 145) betriebsbereit.



Arne Beurling (1905–1986)

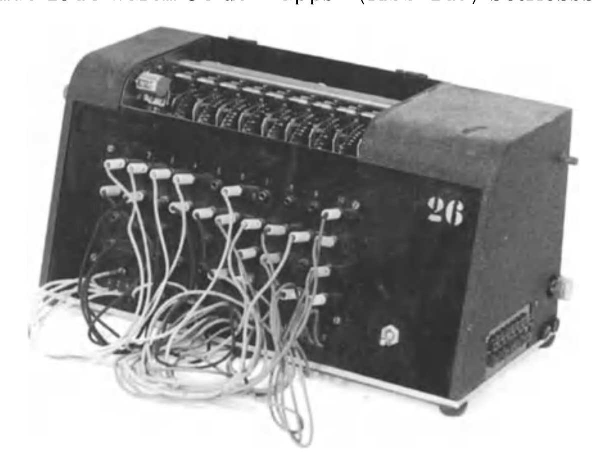


Abb. 145. Vom schwedischen Entzifferungsdienst FRA nachgebauter 'Geheimschreiber'

Am 17. Juni 1942 schöpften die Deutschen aufgrund finnischer Mitteilungen Verdacht, unternahmen aber nicht viel. Die Schweden konnten im Juli 1942 auch noch in den gerade aufgenommenen T52c-Verkehr eindringen. Der Erfolg endete erst im Mai 1943, als die Deutschen die Spruchschlüssel-Prozedur änderten.

19.3 Phasenrichtige Superimposition von überchiffriertem Code

In den bisherigen Beispielen war die Superimposition banal: Die Geheimtexte waren ‚in Phase'. Sind aber zwei oder mehrere Geheimtexte mit verschiedenen Anfangsstellungen eines maschinell erzeugten Schlüssels chiffriert, so müssen sie zuallererst gegenseitig ausgerichtet werden, um eine phasenrichtige Superimposition zu ermöglichen. Dazu kann wie in Kapitel 17 etwa eine Kappa-Untersuchung dienen: Die Geheimtexte sind vermutlich in Phase, sobald ihr gegenseitiges Kappa maximal wird und in der Nähe von κ_S liegt.

19.3.1 Manchmal geht es jedoch auch einfacher. Sofern man bei der Überchiffrierung von Code einen vorbereiteten Schlüssel verwendet, der häufig wechselt, wehrt man den Angriff mit banaler Superimposition gern dadurch ab, daß man für jeden Spruch einen anderen Beginn im Schlüsselmaterial nimmt. Um dazu nicht von vornherein eine Prozedur festlegen zu müssen, hat es sich mancherorts eingebürgert, dem Spruch einen **Spruchschlüssel** (engl. *indicator*, frz. *clef de message*)[7] voranzuschicken, aus dem der Start – sei es Seite, Zeile und Spalte in einem Buch, sei es eine Grundstellung einer Überchiffrierungsmaschine – hervorgeht. Das verbirgt den Schlüssel, aber es kann – was leicht übersehen wird – nicht eine phasenrichtige Ausrichtung der einzelnen Sprüche durch geeignete Methoden (s. o.) verhindern. Im Hinblick auf eine Superimposition ist dies ohnehin nur eine *complication illusoire*, sobald aus den Indikatoren zweier Nachrichten ihre Phasendifferenz direkt festgestellt werden kann.[8] *Kahn* gibt hierfür ein amateurhaftes Beispiel:

Die Überchiffrierungszahlen für einen vierstelligen Code seien vierstellig, ein ebenfalls vierstelliger Indikator ist jedem Spruch vorangestellt, wobei etwa 6218 bedeute: Die ersten vier Zeichen auf Seite 62, Zeile 18. Dann werden die nachrichtentragenden Teile der folgenden fünf Sprüche

(i)	6218	6260	7532	8291	2661	6863	2281	7135	5406	7046	9128	....
(ii)	6216	3964	3043	1169	5729	3392	1952	7572	2754	7891	6290	....
(iii)	6218	4061	6509	4513	1881	0398	3402	8671	4326	8267	6810	....
(iv)	6218	5480	9325	3811	4083	5373	4882	8664	8891	6337	5914	....
(v)	6217	7260	8931	8100	5787	6807	2471	0480	9892	1199	8426	....

phasenrichtig ausgerichtet:

[7] Nicht zu verwechseln mit Kenngruppe (engl. *discriminant*), die Hinweise auf die organisatorische Behandlung der Nachricht gibt.

[8] Um dies zu verhindern, wird der Indikator selbst chiffriert, wie z.B. bei der ENIGMA-Chiffrierung.

			1	2	3	4	5	6	7	8	9	10	.....
(i)			6260	7532	8291	2661	6863	2281	7135	5406	7046	9128	....
(ii)	3964	3043	1169	5729	3392	1952	7572	2754	7891	6290	6719	7529	....
(iii)			4061	6509	4513	1881	0398	3402	8671	4326	8267	6810	....
(iv)			5480	9325	3811	4083	5373	4882	8664	8891	6337	5914	....
(v)		7260	8931	8100	5787	6807	2471	0480	9892	1199	8426	1710	....

Für eine Häufigkeitsanalyse der einzelnen Latten reicht das Material meist nicht aus. Im Falle linearer Substitutionen, insbesondere im vorliegenden Fall einer additiven Überchiffrierung von $\mathbb{Z}_{10}^4$, ist jedoch – wie schon in 18.6.2 – die *symétrie de position* heranziehbar. Die Differenzenmethode bildet dazu wieder für jede Latte Differenzentafeln, etwa für die erste und für die fünfte Latte nach Abb. 146.

1

0000	5101	2209	1880	8339
5909	0000	7108	6789	3238
8801	3902	0000	9681	6130
9220	4321	1429	0000	7559
2771	7872	4970	3551	0000

5

0000	9391	6575	1590	4492
1719	0000	7284	2209	5101
4535	3826	0000	5025	8927
9510	**8801**	5085	0000	3902
6618	5909	2183	7108	0000

Abb. 146. Differenzentafeln

	Differenz	Latte	Nachrichten
	⋮	⋮	⋮
	8209 = 0480 − 2281	6	(v)−(i)
a→	8801 = 4061 − 6260	1	(iii)−(i)
a→	8801 = 5373 − 7572	5	(iv)−(ii)
	9077 = 6509 − 7532	2	(iii)−(i)
	9106 = 5914 − 6810	10	(iv)−(iii)
b→	9220 = 5480 − 6260	1	(iv)−(i)
b→	9220 = 1881 − 2661	4	(iii)−(i)
	9308 = 3811 − 4513	3	(iv)−(iii)
c→	9391 = 1952 − 2661	4	(ii)−(i)
c→	9391 = 6337 − 7046	9	(iv)−(i)
c→	9391 = 6810 − 7529	10	(iii)−(ii)
	9510 = 5373 − 6863	5	(iv)−(i)
	⋮	⋮	⋮

Abb. 147. Differenzentabelle

Angesichts des Umfangs von zehn Differenzentafeln mit je 20 wesentlichen Einträgen ist es angebracht, alle Differenzen zu ordnen, um mehrfach vorkommende aufzufinden. Abb. 147 zeigt einen geeigneten Ausschnitt aus einer solchen Tabelle.

Subtrahiert man nun in jeder Latte jeweils die Subtrahenden der wiederholt auftretenden Differenzen, so erhält man aus den fünf ausgerichteten Nachrichten die teilweise reduzierten Nachrichten: Wie in Abb. 148 gezeigt, wird für die Differenz 8801 in der Latte 1 *6260* subtrahiert, in der Latte 5 *7572* subtrahiert; gleichermaßen wird für die Differenz 9391 in der Latte 4 *2661* subtrahiert, in der Latte 9 *7046*, in der Latte 10 *7529*. Hier umfassen diese

zwei Subtraktionen bereits die aus der Differenz 9220 herrührenden, was als Bestätigung, daß die Phasen richtig ausgerichtet sind, angesehen werden darf.

Die reduzierten Latten sind in einem monoalphabetisch chiffrierten Zwischentext (vgl. 18.3.2); in einem relativen *placode* abgefaßt, der die Übereinstimmungen aufzeigt (kursiv sind die bereits bestimmten relativen Schlüssel angegeben). Die wiederholt auftretenden *placodes* sind **0000**, **9391**, **5909**, **8801**, **9220**, **9391**.

	1'	2	3	4'	5'	6	7	8	9'	10'	....
(i)	**0000**	7532	8291	**0000**	**9391**	2281	7135	5406	**0000**	2609	....
(ii)	**5909**	5729	3392	**9391**	**0000**	2754	7891	6290	9773	**0000**	....
(iii)	**8801**	6509	4513	**9220**	3826	3402	8671	4326	1221	**9391**	....
(iv)	**9220**	9325	3811	2422	**8801**	4882	8664	8891	**9391**	8495	....
(v)	2771	8100	5787	4246	**5909**	0480	9892	1199	1480	4291	....
	6260			*2661*	*7572*				*7046*	*7529*	

Abb. 148. Teilweise reduzierte Nachrichten

Nicht immer verläuft die Differenzenmethode so erfolgreich wie in diesem Beispiel, in dem die ganze Nachricht – mit Ausnahme der unvollständigen Latten – in relativen *placode* überführt werden kann. Oft entstehen zunächst nur Inseln, die sich bei Vorliegen weiteren Materials zu Archipeln zusammenschließen. Es kann trotzdem vorkommen, daß nur partielle Lösungen erzielbar sind; auch können falsche Übereinstimmungen auftreten und den Entzifferer zum Narren halten. Beispielsweise ergibt sich die Differenz 1480 nicht nur aus der Latte 9: 1480 = 8426 − 7046, sondern auch aus der Latte 6 : 1480 = 4882 − 3402. Würde man aber die Latte 6 mittels *3402* reduzieren, so bekäme man einen falschen *placode* – der allerdings beim Vorliegen von mehr Material wieder ausgejätet würde.

19.3.2 Im Abstreifen einer Überchiffrierung hatten die Experten im Auswärtigen Amt, *Paschke*, *Kunze*, *Schauffler*, *Langlotz* seit 1921 langjährige Erfahrung. Sie alle traten dem Dienst, den *Kurt Selchow* leitete, 1918 oder 1919 bei. *Adolf Paschke* war nominell Leiter der Sprachengruppe. *Dr. Werner Kunze*, der Mathematiker (damals eine Seltenheit im Dienst), begann 1921, einen überchiffrierten französischen Code anzugehen und rekonstruierte ihn schließlich 1923; er nahm 1927 diese Arbeit wieder auf. Die Entzifferungsgruppe des AA war zunächst getarnt als Unterabteilung Z der Abteilung I, Personal und Haushalt; 1936 änderte eine Umorganisation ihren Namen in Pers Z.

Die mühselige Arbeit von Hand wurde später maschinell unterstützt, halbautomatisiert. Pers Z ließ *Hans-Georg Krug* teils aus Lochkartenmaschinen, teils aus Bauteilen derNachrichtentechnik solche ‚Roboter', wie *Kahn* sie nennt, herstellen. Auf solchen Vorarbeiten bauten *Hans-Kurt Müller*, *Asta Friedrichs* und andere ihre überragende Leistung auf, die Entzifferung des diplomatischen Code der U.S.A. und das Mitlesen ab August 1941 bis in den

Sommer 1943 hinein. *Allen W. Dulles*, damals amerikanischer Geheimdienstchef in Europa, schöpfte keinen Verdacht, bis ihn *Hans Bernd Gisevius*, ein dem deutschen Widerstand verbundener Angestellter im deutschen Konsulat in Zürich, warnte. Bei Chi, der Chiffrierabteilung des OKW, verfolgten die Ingenieure *Wilhelm Rotscheidt* und *Willi Jensen* entsprechende Gedankengänge (s. 18.6.3). Und der B-Dienst der deutschen Kriegsmarine war gegen die britischen *Naval Cyphers* (22.1.1) erfolgreich. Die Alliierten gingen ähnlich vor, und auch manche Dienste der Neutralen. "*The single most common cryptanalytic procedure of the war [was] the stripping of a numerical additive from enciphered code*" (*David Kahn*).

Kunze leistete auch sonst hervorragende Arbeit: er löste 1936 die japanische Rotormaschine (s. 8.5.7) ORANGE und später auch RED. Im Auswärtigen Amt arbeiteten dann im Krieg, zufolge *Otto Leiberich*, zwölf Linguisten (darunter *Cort Rave*, der die Verbindung zu Erich Hüttenhain im kooperierenden OKW Chi hielt) Tag für Tag an der Entzifferung der PURPLE-Sprüche des japanischen Botschafters in Berlin *Hiroshi Oshima*. Reichsaußenminister *Joachim von Ribbentrop* betrachtete Pers Z als spezielle Waffe im Kampf mit seinen Rivalen *Hermann Göring* and *Heinrich Himmler*.

19.4 Geheimtext-Geheimtext-Kompromittierung

Eine schwierige Situation entsteht in der Praxis, wenn eine Nachricht geringfügig verändert nochmals gesendet werden muß, etwa weil ein Tippfehler korrigiert oder eine Zahlenangabe geändert werden soll. Wird beim zweiten Mal der selbe Schlüssel benutzt, entsteht eine Klartext-Klartext-Kompromittierung von der Stelle der Korrektur an, mit allen geschilderten schlimmen Konsequenzen. Wird jedoch beim zweiten Mal ein verschiedener Schlüssel benutzt, entsteht eine Geheimtext-Geheimtext-Kompromittierung bis hin zu der Stelle der Korrektur.

19.4.1 Eine Geheimtext-Geheimtext-Kompromittierung der Schlüssel entsteht ganz allgemein, wenn ein und die selbe Nachricht oder zumindest ein großes Stück davon zwei- oder mehrmals mit jeweils verschiedenen Schlüsseln chiffriert wird. Eine gefährliche Einbruchsmöglichkeit für den unbefugten Entzifferer entsteht, wenn dies im gleichen System geschieht: Sind die entstehenden Geheimtexte systembedingt ‚isomorph' (2.6.3), so sind sie gleich lang, was sehr leicht auffällt. Ein klassisches Beispiel für einen solchen Angriff boten im Dezember 1938 und Januar 1939 Funksprüche des rumänischen Militärattaches in Paris mit seinem Außenministerium, die sich in der Länge nur um zwei Fünfergruppen unterschieden. Nach *Hüttenhain* gelang es, die Sprüche zu entziffern, wobei sich herausstellte, daß lediglich das Textstück /Heft 17/ des ersten Textes durch das Textstück /Heft 15 statt 17/ im zweiten Text ersetzt war.

Geheimtext-Geheimtext-Kompromittierung der Schlüssel ist geradezu systemimmanent bei vernetzten Nachrichtenverbindungen, wenn ein „Rund-

schreiben“ abgesetzt wird, möglicherweise an Dutzende oder Hunderte von Empfängern, von denen jeder seinen eigenen Schlüssel hat. Konteradmiral *Ludwig Stummel*, für die Sicherheit des Funkverkehrs der Marine verantwortlich, führte 1943 eine Vielzahl von Schlüsselnetzen ein und gab ab Mitte 1944 jedem Unterseeboot seinen eigenen Schlüssel. Das gab den Briten zwar vermehrte Arbeit, stellte sich aber im übrigen als *self-defeating complication* heraus: “*... was actually helpful, because the same message would often appear in several keys, sometimes on different days*” (*Rolf Noskwith*). Selbst *Stummel* hatte es nicht geschafft, Tagesbefehle für jedes Netz oder gar für jedes Boot individuell abzufassen.

Als am 1. Februar 1942 die 4-Rotor-ENIGMA nur für die Unterseeboote eingeführt worden war, kamen häufig Kompromittierungen dadurch zustande, daß allgemeine Befehle für die übrigen Schiffe mit der 3-Rotor-ENIGMA chiffriert übermittelt werden mußten. Hier wäre die Warnung angebracht gewesen, die schon 1914 *Sir Alfred Ewing* formuliert hatte: “*It is never wise to mix ciphers. Like mixing your drinks, it may lead to self-betrayal*”. Aber der Stab von Großadmiral *Dönitz* nahm davon keine Kenntnis.

Streng genommen kann von einer ‚Kompromittierung' der Schlüssel keine Rede mehr sein, wenn die Schlüssel ohnehin öffentlich aind (10.1.2). Jedoch ist nur der Chiffrierschlüssel öffentlich, nicht der Dechiffrierschlüssel, und auf den Dechiffrierschlüssel kommt es ja an. Tatsächlich birgt auch ein öffentliches Chiffrierverfahren inhärent die Gefahr einer Geheimtext-Geheimtext-Kompromittierung des Dechiffrierschlüssels.

Im Jargon von *Bletchley Park* hieß eine Geheimtext-Geheimtext-Kompromittierung der Schlüssel ein ‘*kiss*’. Besser hätte man das Entzücken der Entzifferer über einen solchen Glücksfall nicht ausdrücken können. Die Briten profitierten unter anderem davon, daß kleinere Boote der deutschen Kriegsmarine nicht mit ENIGMAs ausgerüstet waren, sondern auf eine einfache Bigramm-Chiffrierung (‚Werftschlüssel‘) angewiesen waren. Die großen Schiffe dagegen hatten diese Chiffre nicht verfügbar. Wenn nun gewisse Warnungen – beispielsweise vor Treibminen – schnell abzusetzen waren, nahm sich niemand die Mühe, die Klartexte umzuformulieren. Die Briten provozierten gelegentlich solche Vorfälle, um die Geheimtext-Geheimtext-Kompromittierung der schwierig zu brechenden Marine-ENIGMA durch die inzwischen gebrochene simple Bigrammsubstitution herbeizuführen; mit ihrem grimmigem Humor nannten sie das ‘*gardening*’ („Gartenpflege“).

Nachdem am 7. Mai 1941 durch die Aufbringung des Wetterschiffs *München* der ‚Wetterkurzschlüssel‘ in britische Hände gefallen war, ergaben sich aus den Wettermeldungen der Unterseeboote laufend zahlreiche ‘*kisses*’, die die ‘*cribs*’ von *Bletchley Park* füllten, und das hielt an bis 1944. Die Bridgespieler dort nannten das ‘*cross-ruffs*’[9]. Die Aufbringung von *U-559* am 30. Oktober

---

[9] Die Alliierten hatten Erfahrung: Ein ‘cross-ruff’ gelang *J. Rives Childs*, G.2 A.6, A.E.F. im Juli 1918 mit dem Telegramm *Mackensens* über den Rückzug der deutschen Truppen in Rumänien.

1942 ergab sogar eine Kompromittierung der neuen 4-Rotor-ENIGMA durch Wettermeldungen.

Aber auch die Nebeneinanderverwendung einer Überchiffrierung von Code mit Hilfe eines maschinell erzeugten Einmal-Schlüssels einerseits, eines wiederholt verwendeten Additivs andrerseits stellt, wenn letztere Chiffrierung bereits gebrochen ist, den ‚individuellen' Schlüssel bloß und erlaubt die Rekonstruktion der ihn erzeugenden Maschine. Dieses Mißgeschick widerfuhr dem Auswärtigen Amt, das wohl wegen mangelnden Schlüsselnachschubs auf der Strecke Berlin-Dublin die FLORADORA-Überchiffrierung einsetzte, die von den Briten (9.2.1) bereits gebrochen war. Der Schlüssel konnte so untersucht werden, es stellte sich heraus, daß er mittels einer umgebauten Lorenz SZ40 (die die Briten ebenfalls rekonstruiert hatten) erzeugt worden war. Der gesamte für unbrechbar gehaltene Verkehr des AA war damit aufgerollt.

19.4.2 Im Falle einer Chiffrierung mit VIGENÈRE-Schritten, insbesondere auch für überchiffrierten Code, führt eine Geheimtext-Geheimtext-Kompromittierung sofort auf eine Klartext-Klartext-Kompromittierung: Man betrachtet den Klartext als Schlüssel und die Schlüssel als Klartexte. Damit sind die Methoden der Superimposition und der *symétrie de position* anwendbar. Die polyalphabetische Chiffrierung braucht dabei nicht einmal periodisch zu sein. Voraussetzung für einen Erfolg dieses „Rollenwechsels" ist allerdings, daß die Schlüssel in Prosa sind und Häufigkeitsmerkmale zeigen.

Beispielsweise seien die folgenden fünf gleichlangen Nachrichten aufgefangen worden

	1 2 3 4 5	6 7 8 9 10	11 12 13 14 15	16 17 18 19 20	21 22 23 24 25	26 27 28 29 30
(i)	T C C V L	E S K P T	X M P V W	H Y M V G	X B O R V	C W A R F
(ii)	V L L B V	C K W F P	E H E C F	C G N Z E	K K K V I	H D D I D
(iii)	M Y Y R D	M J W M C	U I G L O	K M X L R	E W H X M	R J H A S
(iv)	B K Q T Z	B Z W K W	Z X G Z O	V T B A T	K W M G M	R J K L P
(v)	M Y Y V H	B W J D X	C P C Z O	H V T S I	V M E B S	O H R A U

	31 32 33 34 35	36 37 38 39 40	41 42 43 44
(i)	R R D Y C	T K L B L	M G L W
(ii)	S V F K Q	A J V C R	F K L K
(iii)	H B R N U	T R V G J	X J P W
(iv)	K O W H U	C B D U F	T V E F
(v)	S D A N I	T Y H F K	Z Z W G

und es sei den Umständen nach eine lineare Substitution zu erwarten. Es werden dann in den einzelnen Latten die Differenzen über $\mathbb{Z}_{26}$ aufgestellt. Sechs dieser Aufstellungen zeigen insbesondere Übereinstimmungen in den Differenzen 4, 7 und 11, wie Abb. 149 zeigt. Dabei kommt für Latte 18 nur die fett angegebene 11 als Summe von 4 und 7 in Frage, in Latte 1 kommt 11 nicht in Frage, da 11 und 19, das Komplement von 7, in einer Zeile stehen.

Von den in Latte 36 weiter auftretenden Differenzen finden sich 2 und 9 auch in Latte 1, 2 überdies in Latte 13, 9 in Latte 22. In der Differenzentafel von Latte 13 sind die beiden Differenzen 2 in der zweiten Spalte von der Differenz

1

0	24	**7**	18	**7**
2	0	**9**	20	**9**
19	17	0	11	0
8	6	15	0	15
19	17	0	11	0

13

0	11	9	9	13
15	0	24	24	**2**
17	**2**	0	0	**4**
17	**2**	0	0	**4**
13	24	22	22	0

18

0	25	15	11	19
1	0	16	12	20
11	10	0	22	**4**
15	14	4	0	8
7	6	22	18	0

22

0	17	5	5	15
9	0	14	14	24
21	12	0	0	10
21	12	0	0	10
11	**2**	16	16	0

27

0	19	13	13	15
7	0	20	20	22
13	6	0	0	**2**
13	6	0	0	**2**
11	**4**	24	24	0

36

0	19	0	17	0
7	0	**7**	24	**7**
0	19	0	17	0
9	**2**	**9**	0	**9**
0	19	0	17	0

Abb. 149. Sechs Differenzentafeln

2 in der fünften Spalte zu unterscheiden; eine dieser Differenzen tritt in der Latte 22 auf. (Überdies stellt sich heraus, daß die Differenzen 9 und 11 in der ersten Zeile von Latte 13 zufällig zustande kommen.)

Nimmt man nun die erste Latte als Bezugspunkt und rückt die anderen fünf Latten aufgrund der festgestellten Differenzen zurecht, so ergibt sich das Grundgerüst

	1′	13′	18′	22′	27′	36′
(i)	T	G	M	M	M	M
(ii)	V	V	N	V	T	T
(iii)	M	X	X	H	Z	M
(iv)	B	X	B	H	Z	V
(v)	M	T	T	X	X	M
	0	*9*	*0*	*15*	*10*	*7*

Dieses Grundgerüst kann nun überprüft werden mittels der Latten 5, 6, 7, 10, 12, 19, 20, 24, 30, 31, 33, 37, 38 : es ergibt sich

	5′	6′	7′	10′	12′	19′	20′	24′	30′	31′	33′	37′	38′
(i)	X	P	T	X	B	H	Z	X	X	W	V	M	B
(ii)	H	N	L	T	W	L	X	B	V	X	A	L	L
(iii)	P	X	K	G	X	X	K	D	K	M	M	T	L
(iv)	L	M	A	A	M	M	M	M	H	P	R	D	T
(v)	T	M	X	B	E	E	B	H	M	X	V	A	X
	14	*15*	*25*	*22*	*11*	*14*	*7*	*20*	*8*	*21*	*5*	*24*	*10*

Das gehäufte Auftreten von vier Zeichen M, T, V, X zeigt, daß wir auf dem richtigen Weg sind.

Die weiteren mehrmals auftretenden Zeichen B, L, A, G, K kann man zur Fortsetzung der Differenzenbildung heranziehen. Damit ergibt sich bereits für 40 der 44 Latten eine Ausrichtung:

	1′	2′	3′	4′	5′	6′	7′	8′	9′	10′	11′	12′	13′	14′	15′	16′	17′	18′	19′	20′	21′	22′
(i)	T	E	B	V	X	P	T	L	U	X	Z	B	G	G	B	G		M	H	Z	X	M
(ii)	V	N	K	B	H	N	L	X	K	T	G	W	V	N	K	B		N	L	X	K	V
(iii)	M	A	X	R	P	X	K	X	B	G	W	X	X	W	T	J		X	X	K	E	H
(iv)	B	M	P	T	L	M	A	X	P	A	B	M	X	K	T	U		B	M	M	K	H
(v)	M	A	X	V	T	M	X	K	I	B	E	E	T	K	T	G		T	E	B	V	X
	0	*24*	*1*	*0*	*14*	*15*	*25*	*25*	*21*	*22*	*24*	*11*	*9*	*15*	*21*	*1*		*0*	*14*	*7*	*0*	*15*

	23′	24′	25′	26′	27′	28′	29′	30′	31′	32′	33′	34′	35′	36′	37′	38′	39′	40′	41′	42′	43′	44′
(i)	O	X	K		M	B	K	X	W	H	Y	L	B	M	M	B	G	Z			A	X
(ii)	K	B	X		T	E	B	V	X	L	A	X	P	T	L	L	H	F			A	L
(iii)	H	D	B		Z	I	T	K	M	R	M	A	T	M	T	L	L	X			E	X
(iv)	M	M	B		Z	L	E	H	P	E	R	U	T	V	D	T	Z	T			T	G
(v)	E	H	H		X	W	T	M	X	T	V	A	H	M	A	X	K	Y			L	H
	0	*20*	*11*		*10*	*25*	*7*	*8*	*21*	*10*	*5*	*13*	*1*	*7*	*24*	*10*	*21*	*12*			*11*	*25*

Die in den Fußzeilen angegebenen Verschiebungen sind zum Zwischentext zu addieren, um den Geheimtext zu ergeben. Sie stellen also selbst eine CAESAR-Chiffrierung des Pseudo-Schlüssels (des ursprünglichen Klartextes) dar, die da lautet:

1 2 3 4 5	6 7 8 9 10	11 12 13 14 15	16 17 18 19 20	21 22 23 24 25	26 27 28 29 30
A Y B A O	*P Z Z V W*	*Y L J P V*	*B ∗ A O H*	*A P A U L*	*∗ K Z H I*

31 32 33 34 35	36 37 38 39 40	41 42 43 44
V K F N B	*H Y K V M*	*∗ ∗ L Z*

Jetzt ist Exhaustion angezeigt: Von den 26 Verschiebungen gibt die folgende, durch Addition von 19 erhaltene, den fragmentarischen englischen Klartext

1 2 3 4 5	6 7 8 9 10	11 12 13 14 15	16 17 18 19 20	21 22 23 24 25	26 27 28 29 30
t r u t h	i s s o p	r e c i o	u ∗ t h a	t i t n e	∗ d s a b

31 32 33 34 35	36 37 38 39 40	41 42 43 44
o d y g u	a r d o f	∗ ∗ e s

der auf *Winston Churchill* zurückgeht.[10] Die fünf Pseudo-Klartexte (die fünf ursprünglichen Schlüssel) können leicht rekonstruiert werden, sie finden sich in einem nicht für Kinder geschriebenen „Kinderbuch“:

“*Alice was beginning to get very tired of sitting by he[r sister on the bank ...]*”
“ ‘*Curiouser and curiouser!*’ *cried Alice (she was so much s[urprised ...]*)”
“*They were indeed a queer-looking party that assemble[d on the bank ...]*”
“*It was the White Rabbit, trotting slowly back again, an[d looking ...]*”
“*The Caterpillar and Alice looked at each other for so[me time in silence ...]*”

19.5 Eine Methode von Sinkov

19.5.1 Im Falle periodischer Chiffrierung ist auch bei unabhängigen Alphabeten eine Methode von *Sinkov* anwendbar, die bereits beim Vorliegen von zwei Nachrichten mit gleichem Klartext funktionieren kann.

---

[10] Das komplette Zitat, aus *Churchills* Autobiographie von 1949, lautet “In war-time, thruth is so precious that she should always be attended by a bodyguard of lies” (*Churchill* an *Roosevelt* und *Stalin*).

Folgendes Beispiel von *Sinkov* zeigt das Vorgehen: Die beiden aufgefangenen Nachrichten aus dem Milieu der U.S. Regierung seien:

(i) WCOAK TJYVT VXBQC ZIVBL AUJNY BBTMT
JGOEV GUGAT KDPKV GDXHE WGSFD XLTMI
NKNLF XMGOG SZRUA LAQNV IXDXW EJTKI
YAOSH NTLCI VQMJQ FYYPB CZOPZ VOGWZ
KQZAY DNTSF WGOVI IKGXE GTRXL YOIP

(ii) TXHHV JXVNO MXHSC EEYFG EEYAQ DYHRK
EHHIN OPKRO ZDVFV TQSIC SIMJK ZIHRL
CQIBK EZKFL OZDPA OJHMF LVHRL UKHNL
OVHTE HBNHG MQBXQ ZIAGS UXEYR XQJYC
AIYHL ZVMQV QGUKI QDMAC QQBRB SQNI

Da die beiden Geheimtexte gleich lang sind, drängt sich ein Verdacht auf gleichen Klartext auf. Zunächst ist aber eine Periodenanalyse angebracht: Sie ergibt, daß der erste Geheimtext vermutlich die Periode sechs, der zweite die Periode fünf hat. In diesem Fall ist 30 eine beiden (unbekannten) Schlüsseln gemeinsame Periode. Damit sollte mit jeder Zeichenkoinzidenz zwischen den beiden Texten auch im Abstand von 30 eine Zeichenkoinzidenz auftreten. Tatsächlich zeigt sich in der obigen Aufschreibung in 30 Kolonnen eine Übereinstimmung der beiden 12. Kolonnen und der beiden 15. Kolonnen. Diese Beobachtung stärkt die Vermutung, daß beiden Geheimtexten ein und der selbe Klartext zugrunde liegt, sehr. Nun ist aber

$$12 + 30i = \begin{cases} 6 \pmod 6 \\ 2 \pmod 5 \end{cases}, \qquad 15 + 30i = \begin{cases} 3 \pmod 6 \\ 5 \pmod 5 \end{cases}.$$

Damit steht zu vermuten, daß das 6. Alphabet der ersten Nachricht mit dem 2. Alphabet der zweiten Nachricht und das 3. Alphabet der ersten Nachricht mit dem 5. Alphabet der zweiten Nachricht übereinstimmt. Eine Berechnung von *Chi* gibt hohe Werte, die das erhärten.

Sinkovs Methode zerlegt nun die beiden Nachrichten nach den verwendeten Schlüsseln, die mit α, β, γ, δ, ϵ, ζ und ι, κ, λ, μ, ν bezeichnet werden sollen – der Anfang dieser Zerlegung lautet

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
α	W						J						B						B						Y					
β		C						Y						Q						L						B				
γ			O						V						C						A						B			
δ				A						T						Z						U						T		
ϵ					K						V						I						J						M	
ζ						T						X						V						N						T
ι	T					J					M					E					E					D				
κ		X					X					X					E					E					Y			
λ			H					V					H					Y					Y					H		
μ				H					N					S					F					A					R	
ν					V					O					C					G					Q					K

In dieses Diagramm können nun weitere Einträge gemacht werden: Da beide Chiffren zum selben Klartext gehören, können die 2., die 7. und die 12. Spalte, die übereinstimmend X für den Schlüssel κ zeigen, überlagert werden. Ebenso können die 3., die 13. und die 28. Spalte, die übereinstimmend H für den Schlüssel λ zeigen, überlagert werden, desgleichen die 16. und 21. Spalte (E für den Schlüssel ι), die 17. und 22. Spalte (E für den Schlüssel κ), die 18. und 23. Spalte (Y für den Schlüssel λ). Damit ergibt sich bereits folgendes Bild

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
α	W	J	B				J					J	B						B						Y			B		
β		C					C	Y				C		Q						L						B				
γ			O						V				O		C	A					A						B	O		
δ			T	A						T			T			Z	U				Z	U						T		
ϵ					K						V						I	J				I	J						M	
ζ		X				T	X					X						V					V	N						T
ι	T					J					M					E					E					D				
κ		X					X					X					E					E					Y			
λ			H					V					H					Y					Y					H		
μ				H					N					S					F					A					R	
ν					V					O					C					G					Q					K

Diese **Überlagerung** erstreckt sich natürlich auf die ganze Länge der beiden Nachrichten. In gleicher Weise kann die Überlagerung auch in die Zeilen ι, κ, λ, μ, ν gehen: Die dreizehnte und die neunzehnte Spalte, die übereinstimmend B für den Schlüssel α zeigen, können überlagert werden usw. Insgesamt ergibt sich so über die volle Länge 149 der Nachrichten folgende Aufstellung

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
α	W	J	B	M		D	J	P		B		J	B	W	M	J		N	B	U	J		N	X	Y		L	B	J	D
β	Q	C	K	E	X		C	Y	X	K		C	K	Q	E	C		A	K	L	C		A		T	B		K	C	
γ	L	A	O	C	V	K	A	W	V	O	N	A	O	L	C	A		Z	O	G	A		Z		Q	S	B	O	A	K
δ	G	Z	T	A	F		Z		F	T		Z	T	G	A	Z	U	X	T	I	Z	U	X		L			T	Z	
ϵ	Y	M	D	R	K	F	M		K	D	V	M	D	Y	R	M	I	J	D	W	M	I	J		S			D	M	F
ζ	I	X	Q	Z	D	T	X		D	Q		X	Q	I	Z	X	E	V	Q	P	X	E	V	N	G		Y	Q	X	T
ι	T	E		U	Z	J	E	S	Z		M	E		T	U	E		C		Q	E		C	H	O	D			E	J
κ	I	X	Q	Z	D	T	X		D	Q		X	Q	I	Z	X	E	V	Q	P	X	E	V	N	G		Y	Q	X	T
λ	J	S	H	B			S	V		H	I	S	H	J	B	S		Y	H	N	S		Y		M		A	H	S	
μ	S	R	F	H	N		R	G	N	F		R	F	S	H	R		M	F	Y	R		M	A	B	Q		F	R	
ν	L	A	O	C	V	K	A	W	V	O	N	A	O	L	C	A		Z	O	G	A		Z		Q	S	B	O	A	K
$\to$	A	B	C	H	D	E	B	F	D	C	G	B	C	A	H	B	I	J	C	K	B	I	J	L	Q	M	N	C	B	E

	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
α	J		B			Y	U		J	B			P	B		W	B	J	H	M	P	W	Y		D		W	B	J	W
β	C	G	K			T	L	G	C	K	X	X	Y	K	X	Q	K	C		E	Y	Q	T			X	Q	K	C	Q
γ	A		O		N	Q	G		A	O	V	V	W	O	V	L	O	A		C	W	L	Q		K	V	L	O	A	L
δ	Z		T	E		L	I		Z	T	F	F		T	F	G	T	Z	E	A		G	L			F	G	T	Z	G
ϵ	M		D	P	V	S	W		M	D	K	K		D	K	Y	D	M	P	R		Y	S		F	K	Y	D	M	Y

```
ζ   XHQ    GPHXQ  DD QD  IQX Z   IGFT  DIQXI
ι   E   M  OQ E   ZZS Z  T E U  STO J  ZT ET
κ   XHQ    GPHXQ  DD QD  IQX Z   IGFT  DIQXI
λ   SKH    MNKSH    VH   JHS B  VJM     JHSJ
μ   R FI   BY RF  NNGFN  SFRIH  GSBJ   NSFRS
ν   A O N  QG AO  VVWOV  LOA C  WLQ K  VLOAL

→   BOCPG  QKOBC  DDFCD  ACBPH  FAQRE  DACBA

    6162636465 6667686970 7172737475 7677787980 8182838485 8687888990

α   NB YD  JM BW  YMR J  Y BN    NBJW  M B W
β   AK T   CEGKQ  TE UC  T KAV   AKCQ  E KXQ
γ   ZONQK  AC OL  QC  A  Q OZF  IZOAL  CJOVL
δ   XT L   ZA TG  LA  Z  L TX    XTZG  A TFG
ε   JDVSF  MR DY  SR  M  DADJ    JDMY  R DKY
ζ   VQ GT  XZHQI  GZ  X  GJQV    VQXI  ZKQDI
ι   C MOJ  EU  T  OU  E  O  CX  LC ET  U  ZT
κ   VQ GT  XZHQI  GZ  X  GJQV    VQXI  ZKQDI
λ   YHIM   SBKHJ  MBD S  M HY    YHSJ  B H J
μ   MF B   RH FS  BH PR  B FMK   MFRS  H FNS
ν   ZONQK  AC OL  QC  A  Q OZF  IZOAL  CJOVL

→   JCGQE  BHOCA  QHSTB  QUCJV  WJCBA  HXCDA

    9192939495 9697989900 0102030405 0607080910 1112131415 1617181920

α   YNB    XTUMU   BM Y   WLP   MJ UZ   BWUM
β   TAK      LEL   KEJT  XQ YB  EC L   VKQLE
γ   QZO E    GCG  NOC Q  VLBWS  CA GR  FOLGC
δ   LXTS     IAI   TA L  FG     AZ I    TGIA
ε   SJD H    WRW  VDR S  KY     RMOW    DYWR
ζ   GVQ    NBPZP   QZ G  DIY    ZX P    QIPZ
ι   OC     H QUQ  M U O  ZT SD  UE Q   X TQU
κ   GVQ    NBPZP   QZ G  DIY    ZX P    QIPZ
λ   MYH      NBN  IHB M   JAV   BSEN    HJNB
μ   BMFT   A YHY   FHXB  NS GQ  HR Y   KFSYH
ν   QZO E    GCG  NOC Q  VLBWS  CA GR  FOLGC

→   QJCYZ  L1KHK  GCH2Q  DANFM  HB3K4  VCAKH

1.. 2122232425 2627282930 3132333435 3637383940 4142434445 46474849

α   KWNMW   NY    UYO    U YXM  UBMJL  PBU
β    QAEQ  XATBX  LT VG  LXT E  LKEC   YKL
γ    LZCL  VZQSV  GQ FI  GVQ C  GOCAB  WOG
δ    GXAG  FXL F  IL     IFL A  ITAZ    TIE
ε    YJRY  KJS K  WS     WKS R  WDRM    DWP
ζ    IVZI  DVG D  PG  H  PDGNZ  PQZXY   QP
ι   ATCUT  ZCODZ  QO X   QZOHU  Q UE   S Q
κ    IVZI  DVG D  PG  H  PDGNZ  PQZXY   QP
λ    JYBJ   YM    NMU K  N M B  NHBSA  VHN
μ    SMHS  NMBQN  YB K   YNBAH  YFHR   GFYI
ν    LZCL  VZQSV  GQ FI  GVQ C  GOCAB  WOG

→   5AJHA  DJQMD  KQ6VO  KDQLH  KCHBN  FCKP
```

Erwartungsgemäß sind die mit den Schlüsseln ζ und κ bezeichneten Zeilen identisch, desgleichen die mit den Schlüsseln γ und ν bezeichneten[11] . Nicht alle Felder sind ausgefüllt, gewisse Spalten wie die achte und die siebzehnte könnten eventuell zusammenfallen. In der Tat kommen 32 verschiedene Spalten vor, die in der mit dem Pfeil $\longrightarrow$ gekennzeichneten Zeile in willkürlicher Weise mit den Zeichen A ... Z und 1 ... 6 bezeichnet werden. 32 Spalten – das sind mehr, als zu den höchstens 26 Alphabetzeichen gehören. Gewisse Spalten bedeuten also das selbe Klartextzeichen: Wir haben eine monoalphabetische Chiffrierung erreicht, aber eine mit Homophonen. Glücklicherweise wird sich herausstellen, daß nicht – wie es zur Erschwerung der unbefugten Entzifferung gemacht wird – die häufigen Zeichen von der Homophonie betroffen sind, sondern gerade die seltenen; sie bieten nämlich mit ihrem seltenen Vorkommen nicht genügend Material zur Auffüllung der Felder.

19.5.2 Die nunmehr erzielte monoalphabetische Chiffre

```
ABCHD EBFDC GBCAH BIJCK BIJLQ MNCBE
BOCPG QKOBC DDFCD ACBPH FAQRE DACBA
JCGQE BHOCA QHSTB QUCJV WJCBA HXCDA
QJCYZ L1KHK GCH2Q DANFM HB3K4 VCAKH
5AJHA DJQMD KQ6VO KDQLH KCHBN FCKP
```

zeigt deutlich die Häufigkeitsverteilung des Englischen, mit einem herausragenden C und etwa gleichhäufigen B, A, H, D, O, N . Als Einstiegshilfe mag nun dienen das wahrscheinliche Wort /treasurysecretary/ mit dem Muster *1234562753823142 7* . Es paßt genau auf den Anfang. Damit hat man mit acht Buchstaben schon viel erreicht:

```
treas uryse creta rIJeK rIJLQ MNeru
rOePc QKOre ssyes terPa ytQRu stert
JecQu raOet QaSTr QUeJV WJert aXest
QJeYZ L1KaK cea2Q stNyM ar3K4 VetKa
5tJat sJQMs KQ6VO KsQLa KearN yeKP
```

Sofort ins Auge springt das Wort /yesterday/ in der zweiten Zeile, was aber nicht viel bringt, und davor das Wort /congress/ . Damit sind vier weitere Buchstaben bestimmt und vom *etaonirsh* fehlen nur noch das /i/ und das /h/. Es ergibt sich

```
treas uryse creta rIJen rIJLo MNeru
rgedc ongre ssyes terda ytoRu stert
Jecou raget oaSTr oUeJV WJert aXest
oJeYZ L1nan cea2o stNyM ar3n4 Vetna
5tJat sJoMs no6Vg nsoLa nearN yend
```

Nun bedeutet vermutlich I homophon mit F den Buchstaben /y/ , in der ersten Zeile liest man dann /henry/ . Mit dem /i/ hat man Schwierigkeiten,

[11] Bei manueller Arbeit wird man diese Zeilen nur einmal anschreiben, bei programmierter Durchführung ist es dagegen organisatorisch einfacher, sie zu wiederholen.

in der letzten Zeile könnte man /no signs/ lesen, wenn 6 homophon mit D den Buchstaben /s/ bedeutete. Jetzt hat man

```
t r e a s   u r y s e   c r e t a   r y h e n   r y h L o   M N e r u
r g e d c   o n g r e   s s y e s   t e r d a   y t o R u   s t e r t
h e c o u   r a g e t   o a S T r   o U e h i   W h e r t   a X e s t
o h e Y Z   L 1 n a n   c e a 2 o   s t N y M   a r 3 n 4   i e t n a
5 t h a t   s h o M s   n o s i g   n s o L a   n e a r N   y e n d
```

und liest in der zweiten Zeile /to muster/, in der dritten Zeile /approve higher taxes/ (S und T homophon), in der vierten Zeile /help finance a costly war in vietnam/ , womit sich schließlich in der ersten Zeile der Name /henry h fowler/ und insgesamt als Klartext ergibt

```
t r e a s   u r y s e   c r e t a   r y h e n   r y h f o   w l e r u
r g e d c   o n g r e   s s y e s   t e r d a   y t o m u   s t e r t
h e c o u   r a g e t   o a p p r   o v e h i   g h e r t   a x e s t
o h e l p   f i n a n   c e a c o   s t l y w   a r i n v   i e t n a
m t h a t   s h o w s   n o s i g   n s o f a   n e a r l   y e n d
```

Die Chiffriertabelle lautet unter Einbeziehungen der Überlagerungen, die sich aus den festgestellten Homophonen ergeben, aber unter Offenlassung der fehlenden Buchstaben — aus den 32 Spalten werden 21 Zeichen:

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
α	M				B	X		N	T			L	K	U	Y	R		J	O	W	D	Z			P	
β	E		J		K		G	A	V					L	T	U		C	X	Q			B		Y	
$\gamma=\nu$	C		N		O		I	Z	F			B		G	Q	E		A	V	L	K	R	S	J	W	
δ	A			E	T			X				S		I	L			Z	F	G					U	
ϵ	R		V	P	D			J	O					W	S	H		M	K	Y	F	A			I	
$\zeta=\kappa$	Z				Q	N	H	V	B			Y	F	P	G			X	D	I	T	J		K	E	
ι	U		M			H	L	C	X				A	Q	O			E	Z	T	J		D		S	
λ	B		I		H		K	Y	E			A		N	M	D		S	U	J					V	
μ	H		X	I	F	A		M	K			T	J	Y	B	P		R	N	S			Q		G	
	H		G	P	C	L	O	J	V			N	R	K	Q	S		B	D	A	E	U	M	X	F	
$\rightarrow$			2				W		1			Y	5			T			6			4			I	
									3							Z										

19.5.3 Die vollständige Chiffriertabelle kann man gewinnen, wenn es sich um verschobene Alphabete handeln sollte. Dies ist tatsächlich der Fall, und mit der in 18.8.2 angesprochenen Methode von *Friedman* gelingt es, das Referenzalphabet zu rekonstruieren. Zur Entzifferung brauchte man aber von dieser speziellen Eigenschaft gar keinen Gebrauch zu machen.

Zunächst geht *Friedman* von der begründeten Annahme aus, daß in der zu suchenden Chiffriertabelle alle Spalten aus einer einzigen durch zyklische Verschiebung hervorgehen (7.2.1, 8.2.3). Greift man nun etwa die Zeilen λ und μ heraus, so finden sich in einem noch unbekannten Abstand k unter /t/ die Buchstaben J und S , unter /r/ S und R , ferner N und Y , Y und M , M und B , B und H , H und F , V und G . Wir haben also bereits drei Ketten

J-S-R , N-Y-M-B-H-F und V-G

von Buchstaben im Abstand k. Aber auch in den Zeilen α und λ finden sich unter /r/ die Buchstaben J und S; somit stehen im gleichen Abstand k auch die Buchstaben W und J, R und D, O und U, U und N, P und V, L und A. Die vorhandenen Ketten lassen sich verlängern, neue lassen sich bilden; wir haben jetzt

W-J-S-R-D , O-U-N-Y-M-B-H-F , P-V-G und L-A .

J und D haben den Abstand $3k$; in den Zeilen ι und α finden sich unter /u/ die Buchstaben J und D , also haben nicht nur U und M, O und Y, sondern auch C und N, X und T, A und K, Q und U, E und J, Z und O, T und W, S und P diesen Abstand. Damit ergeben sich die Ketten

T-E-∗-W-J-S-R-D-P-V-G , Q-C-O-U-N-Y-M-B-H-F-∗-X , L-A-∗-∗-K .

Der Zusammenschluß dieser Ketten gelingt nun mit der Beobachtung, daß W und G , die sich in den Zeilen α und δ finden, den Abstand $7k$ haben, damit haben diesen Abstand auch J und Z, B und T, M und A, U und I, H und E, Y und L, womit sich der Zykel schließt:

T-E-K-W-J-S-R-D-P-V-G-Z-Q-C-O-U-N-Y-M-B-H-F-I-X-L-A- .

Dies braucht jedoch, vgl. 18.8.1, noch nicht die ursprüngliche Reihenfolge zu sein. Bildet man potenzierte Zyklen, so wird man mit der fünften Potenz

T-S-G-U-H-A-J-V-O-B-L-W-P-C-M-X-K-D-Q-Y-I-E-R-Z-N-F-

fündig; die Folge

H A J V O B L W P C M X K D Q Y I E R Z N F T S G U

ergibt sich – spaltenweise – aus dem Kennwort HOPKINS durch die in 3.2.5 beschriebene Methode:

H	O	P	K	I	N	S
A	B	C	D	E	F	G
J	L	M	Q	R	T	U
V	W	X	Y	Z		.

Mit dieser Folge bildet man eine *tabula recta*. Zur Bestimmung der Kopfzeile verfährt man folgendermaßen: Eine „fette" Zeile wie die mit $\gamma = \nu$ bezeichnete lautet umgeordnet

	r	x	s	e	l	t	y		a			u		o		g	p	v	h	c	i			w	n	
$\gamma = \nu$	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U

Die anderen bisher betrachteten Zeilen fügen sich ein und legen weitere Klartextzeichen fest. Man erhält insgesamt eine permutierte Kopfzeile

∗ r x s e l t y ∗ a f m u ∗ o ∗ g p v h c i ∗ w n d

die lediglich noch nicht die fünf fehlenden, seltenen Klartextzeichen /b/, /j/, /k/, /q/, /z/ umfaßt. Diese Kopfzeile verrät schließlich auch ihr Kennwort: Sie entsteht mit der Konstruktion von 3.2.5 aus dem Kennwort /johns/ .



j o h n s
a b c d e
f g i k l
m p q r t
u v w x y
z .

Damit sind auch die noch fehlenden Klartextzeichen erfaßt. Die sich ergebende Chiffriertabelle (*tabula recta*) zeigt Tabelle 26. Sie fällt unter das Stichwort ‚dreifache Chiffrierung' (8.2.3). Die Kennwörter /johns/ and HOPKINS zur Bildung der Alphabete sind offensichtlich eine Anspielung auf Johns Hopkins (1795–1873), amerikanischer Finanzier und Philanthrop.[12]
Die Schlüssel sind passenderweise *CIPHER* und *GROUP*, wie man aus den Eingängen für $\alpha\beta\gamma\delta\epsilon\zeta$ und $\iota\kappa\lambda\mu\nu$ in Tabelle 26 entnehmen kann.

		j	a	f	m	u	z	o	b	g	p	v	h	c	i	q	w	n	d	k	r	x	s	e	l	t	y
δ	*H*	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U
	A	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H
	J	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A
	V	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J
λ	*O*	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J	V
	B	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J	V	O
	L	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J	V	O	B
	W	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J	V	O	B	L
$\gamma=\nu$	*P*	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J	V	O	B	L	W
α	*C*	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J	V	O	B	L	W	P
	M	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J	V	O	B	L	W	P	C
	X	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J	V	O	B	L	W	P	C	M
	K	K	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J	V	O	B	L	W	P	C	M	X
	D	D	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J	V	O	B	L	W	P	C	M	X	K
	Q	Q	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J	V	O	B	L	W	P	C	M	X	K	D
	Y	Y	I	E	R	Z	N	F	T	S	G	U	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q
β	*I*	I	E	R	Z	N	F	T	S	G	U	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y
ϵ	*E*	E	R	Z	N	F	T	S	G	U	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I
$\zeta=\kappa$	*R*	R	Z	N	F	T	S	G	U	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E
	Z	Z	N	F	T	S	G	U	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R
	N	N	F	T	S	G	U	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z
	F	F	T	S	G	U	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N
	T	T	S	G	U	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F
	S	S	G	U	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T
ι	*G*	G	U	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S
μ	*U*	U	H	A	J	V	O	B	L	W	P	C	M	X	K	D	Q	Y	I	E	R	Z	N	F	T	S	G

Tabelle 26. Chiffriertabelle mit permutierter Kopfzeile

[12] An der Johns Hopkins University in Maryland, U.S.A. wurde im 2. Weltkrieg die '*proximity fuze*', ein Geschoß mit Näherungszünder, entwickelt.

19.6 Geheimtext-Geheimtext-Kompromittierung: Indikatorverdopplung

"The double encipherment of each text-setting was a gross error."
Gordon Welchman 1982

Die Polen waren für den hohen Standard ihrer kryptanalytischen Fähigkeiten bekannt: Sie hatten mit Hilfe von unbefugten Entzifferungen 1920 den Krieg gegen Rußland gewonnen.

Wie *Władysław Kozaczuk* erst 1967 aufdeckte,[13] ermöglichte ein geradezu typischer Fall einer Geheimtext-Geheimtext-Kompromittierung ab 1932 dem polnischen *Biuro Szyfrów* (Major *Gwido Langer*, 'Luc') mit seinem Dechiffrierdienst B.S.-4 unter Hauptmann *Maksymilian Ciężki* (1899–1951) und den jungen, aus zwei Dutzend Mathematikstudenten ausgewählten Mitarbeitern *Marian Rejewski*, *Henryk Zygalski*, *Jerzy Różycki* das Eindringen in die Chiffrierung der deutschen Wehrmacht. (Funksprüche wurden in den östlichen Provinzen Preußens übungshalber reichlich in den Äther gesetzt.)

Der Ansatz lag zunächst in einer typischen Schwäche der üblichen Schlüsselverwaltung für Chiffriermaschinen mit eigenem Schlüsselerzeuger (8.5): Weil es zu schwierig und fehleranfällig war, für jede Verbindung eine individuelle Ausgangsstellung (‚Grundstellung') der an ihr beteiligten zwei Chiffriermaschinen vorzusehen, die außerdem jeweils nach relativ kurzer Zeit hätte gewechselt werden müssen, führte man (vgl. 19.3.1) **Spruchschlüssel** ein (engl. *indicator*, hier spezifisch *text-setting*, *message-setting*). Für den ENIGMA-Verkehr geschah dies folgendermaßen: Mit einem für den betreffenden Tag gültigen *allgemeinen* ‚Tagesschlüssel', der die Reihenfolge der drei Rotoren (‚Rotorenlage'), die interne ‚Ringstellung' auf jedem einzelnen Rotor, die Steckerverbindung und eine *allgemeine* **Grundstellung** der drei Rotoren beinhaltete, wurde vom Sender als Spruchschlüssel eine 3-Buchstaben-Gruppe frei gewählt und chiffriert abgegeben (**chiffrierter Spruchschlüssel**, engl. *[encrypted] indicator*), die vom Empfänger dechiffriert wurde und für den anschließenden Spruch sender- wie empfängerseitig als Ausgangsstellung der drei Rotoren diente.

Die Chiffrierung des Spruchschlüssels durch die ENIGMA selbst konnte als besonders kluger Einfall gewertet werden; tatsächlich wäre es besser gewesen, ein eigenes Chiffrierverfahren für den Spruchschlüssel vorzusehen – wie es seit 1941 mit einer Bigramm-Chiffrierung für die 4-Rotor-ENIGMA der Marine geschah – aber seine bedingte Offenlegung wurde von den Deutschen als unbedenklich angesehen, da die ROTOR-Chiffrierung als unüberwindbar galt. Niemand schien den *circulus vitiosus* zu bemerken.

[13] Sein Buch *Bitwa o tajemnice* (in polnischer Sprache) wurde im Westen nicht beachtet. Immerhin erschien 1967 eine Rezension in einer Göttinger Zeitschrift. Auch hat schon 1968 *Donald C. Watt* ("Breach of Security", London 1968) darauf hingewiesen, daß 1939 Großbritannien von Polen ENIGMA-Maschinen und -Chiffrierunterlagen erhielt.

Diese Sicherheit in Zweifel ziehend, gelang es dem polnischen Dienst zunächst trotzdem nicht, den 1930 einsetzenden ENIGMA-Funkverkehr mitzulesen, obwohl er sich mit dem Arbeitsprinzip der kommerziellen ENIGMA (7.3.2), die auf dem offenen Markt war, seit 1926 vertraut gemacht hatte. (Die inneren Verbindungen der Rotoren in der militärischen ENIGMA I von 1930 waren anders als in der kommerziellen Ausführung.) Der Einbruch gelang schließlich an einer weiteren Schwachstelle: Weil man im störungsanfälligen Funkverkehr nicht sicher sein konnte, daß der Spruchschlüssel korrekt übertragen würde, übertrug man ihn zweifach – die tückische Vorliebe für kurze Verdopplungen (11.1.5) tobte sich auch hier aus. Hätte man das Chiffrat zweimal nacheinander übertragen, so wäre nicht zu vermeiden gewesen, daß dies dem Gegner auffallen würde und er den Charakter der Spruchschlüsselgruppe erkennen und darauf seinen Angriff richten würde. So glaubte man, den Spruchschlüssel erst verdoppeln und dann chiffrieren zu müssen – und handelte sich damit eine viel schwerer wiegende Geheimtext-Geheimtext-Kompromittierung ein; eine winzige zwar, aber an einem festen Platz. All dies war nicht der ENIGMA-Maschine selbst anzulasten, aber den Regeln für ihren Betrieb. Die Spruchschlüsselverdopplung war auch betrieblich nicht unbedingt nötig: Als sie am 1. Mai 1940 aufgegeben wurde, lief der ENIGMA-Verkehr trotzdem ungestört weiter.

Die schrullige Idee der Verdoppelung des Spruchschlüssels scheint übrigens auf Empfehlungen von 1924 für die kommerzielle ENIGMA zurückzugehen.

Der polnische Dienst hatte überdies rasch herausgefunden, daß zwei Sprüche, die mit der selben 6-Buchstaben-Gruppe begannen, eine erhöhte Zeichenkoinzidenz nahe κ_d aufwiesen, also *superimposition* erlaubten. Somit war durch die erste 6-Buchstaben-Gruppe die Ausgangsstellung der Rotoren festgelegt.

19.6.1 Frankreich I. Hilfe kam für die Polen aus Frankreich. Der bis 1938 in der Chiffrier-Stelle des Reichswehrministeriums tätige Spion *Hans-Thilo Schmidt* (1888–1943, mit Decknamen ASCHE, Asché, frz. *H.E.*), der 23.3.1943 entdeckt und angeblich im Juli hingerichtet wurde (Selbstmord 19.9.1943), hatte seit Oktober 1931 Gebrauchsanleitungen, Schlüsselanleitungen und sogar Tagesschlüssel für September und Oktober 1932 (samt der Ringstellungen und Steckerverbindungen für diese beiden Monate) über den Agenten 'Rex' an den französischen Chiffrierdienstchef 'Bolek', den damaligen Major *Gustave Bertrand* verraten, der das Material an den polnischen Dienst weitergab.

19.6.2 Polen I. *Ciężki*s junger Mitarbeiter, der geniale[14] *Marian Rejewski* (1905–1980) hatte nun jedenfalls herauszufinden, wie man daraus Nutzen

[14] *Marian Rejewski*s intuitive Fähigkeiten werden durch folgende Episode beleuchtet: Bei der kommerziellen ENIGMA waren die Kontakte auf dem Eingangsring in der Reihenfolge der Buchstabenanordnung auf der Tastatur belegt. Das schien bei der militärischen ENIGMA I nicht so zu sein. *Rejewski* sagte sich, „die Deutschen setzen auf Ordnung", versuchte es mit der alphabetischen Reihenfolge (s. 7.3.2) – und gewann. Der britische Kryptanalyst *Knox*, der sich über diese Frage seit langem den Kopf zerbrochen hatte, erfuhr die Lösung erst im Juli 1939 von *Rejewski*, der berichtete "*Knox* was furious when he learned how simple it was".

ziehen konnte. Folgt man dem Bericht von *Kozaczuk* (1984), so ging er folgendermaßen vor: Er vermutete, daß die ihrem Sinn nach frei zu wählenden Spruchschlüssel gewisse charakteristische Abweichungen von der Gleichverteilung aufwiesen – nicht viel anders als die vom Publikum tatsächlich benutzten Lottozahlen. (Die Anweisungen der Deutschen zur Chiffriersicherheit waren in diesem Punkt mangelhaft; so konnte sich ein Nachrichtenoffizier, der den Befehl gegeben hatte, als Spruchschlüssel jeweils die Endstellung der Rotoren nach dem vorangegangenen Spruch zu nehmen, darauf hinausreden, er habe ja dafür gesorgt, daß der Spruchschlüssel stets gewechselt wurde.) Tatsächlich kamen als Spruchschlüssel häufig vor stereotype Dreiergruppen wie aaa , bbb , sss . Als die reine Buchstabenwiederholung Frühjahr 1933 von den Deutschen explizit verboten wurde, war es zu spät. Außerdem kam jetzt die einige Zeit anhaltende Unsitte auf, waagrecht, senkrecht und diagonal auf dem Tastenfeld zu tippen: qwe , asd (horizontal!), qay , cde (vertikal!) etc., womit weiterhin die von *Rejewski* entdeckte Einbruchmöglichkeit bestand.

1.	AUQ	AMN	14.	IND	JHU	27.	PVJ	FEG	40.	SJM	SPO	53.	WTM	RAO
2.	BNH	CHL	15.	JWF	MIC	28.	QGA	LYB	41.	SJM	SPO	54.	WTM	RAO
3.	BCT	CGJ	16.	JWF	MIC	29.	QGA	LYB	42.	SJM	SPO	55.	WTM	RAO
4.	CIK	BZT	17.	KHB	XJV	30.	RJL	WPX	43.	SUG	SMF	56.	WKI	RKK
5.	DDB	VDV	18.	KHB	XJV	31.	RJL	WPX	44.	SUG	SMF	57.	XRS	GNM
6.	EJP	IPS	19.	LDR	HDE	32.	RJL	WPX	45.	TMN	EBY	58.	XRS	GNM
7.	FBR	KLE	20.	LDR	HDE	33.	RJL	WPX	46.	TMN	EBY	59.	XOI	GUK
8.	GPB	ZSV	21.	MAW	UXP	34.	RFC	WQQ	47.	TAA	EXB	60.	XYW	GCP
9.	HNO	THD	22.	MAW	UXP	35.	SYX	SCW	48.	USE	NWH	61.	YPC	OSQ
10.	HNO	THD	23.	NXD	QTU	36.	SYX	SCW	49.	VII	PZK	62.	YPC	OSQ
11.	HXV	TTI	24.	NXD	QTU	37.	SYX	SCW	50.	VII	PZK	63.	ZZY	YRA
12.	IKG	JKF	25.	NLU	QFZ	38.	SYX	SCW	51.	VQZ	PVR	64.	ZEF	YOC
13.	IKG	JKF	26.	OBU	DLZ	39.	SYX	SCW	52.	VQZ	PVR	65.	ZSJ	YWG

Abb. 150. 65 aufgefangene chiffrierte Spruchschlüssel zum gleichen Tagesschlüssel

19.6.2.1 Mit $P_1, P_2, P_3, P_4, P_5, P_6$ (bei *Rejewski* A, B, C, D, E, F) seien die Permutationen bezeichnet, denen bei fester Grundstellung die 1., 2., 3., . . . 6. Zeichen unterliegen. Aus $\mathrm{a}P_i = \mathrm{X}$ und $\mathrm{a}P_{i+3} = \mathrm{Y}$ $(i = 1, 2, 3)$ folgt, daß $\mathrm{X}P_i^{-1}P_{i+3} = \mathrm{Y}$. Der echt involutorische Charakter der ENIGMA-Chiffrierung war aber den Polen bekannt. Damit folgt aus $\mathrm{a}P_i = \mathrm{X}$ und $\mathrm{a}P_{i+3} = \mathrm{Y}$ $(i = 1, 2, 3)$, daß $\mathrm{X}P_iP_{i+3} = \mathrm{Y}$. Die bekannten, an jeweils 1. und 4., 2. und 5., 3. und 6. Stelle des Chiffrats stehenden Zeichen X, Y legen also die drei Produkte P_iP_{i+3} der unbekannten Permutationen fest.

Abb. 150 zeigt 65 chiffrierte verdoppelte Spruchschlüssel. Aus ihnen entnimmt man für P_1P_4 , daß das Zeichen a in sich übergeht (nr 1.), ebenso das Zeichen s (nr 35.). Ferner geht das Zeichen b in c über und umgekehrt (nr 2. , nr 4.), ebenso das Zeichen r in w und umgekehrt (nr 30. , nr 53 .). Von den übrigen Zeichen findet man, daß sie unter P_1P_4 in den Zyklen (d v p f k x g z y o) (etwa nr 5. , nr 49. , nr 27. , nr 7. , nr 17. , nr 57. , nr 8. ,

nr 63., nr 61., nr 26.) und (e i j m u n q l h t) (etwa nr 6., nr 12., nr 15., nr 21., nr 48., nr 23., nr 28., nr 19., nr 9., nr 45.) liegen. Es handelt sich also um zwei Einerzyklen, zwei Zweierzyklen und zwei Zehnerzyklen. Die Zyklenbestimmung ist vollständig möglich, sobald jedes Zeichen an 1., an 2. und an 3. Stelle mindestens einmal aufgetreten ist; in der Regel ist das der Fall, sobald fünfzig bis hundert Sprüche vorliegen – das warf ein heißer Manövertag schon ab. Insgesamt ergibt sich

P_1P_4= (a) (s) (b c) (r w) (d v p f k x g z y o) (e i j m u n q l h t)
P_2P_5= (a x t) (b l f q v e o u m) (c g y) (d) (h j p s w i z r n) (k)
P_3P_6= (a b v i k t j g f c q n y) (d u z r e h l x w p s m o)

Die Einerzyklen[15] (engl. *uniliteral cycle*) spielen eine besondere Rolle: Da die einzelnen Substitutionen P_1, P_2, P_3, P_4, P_5 und P_6 wegen ihres echt involutorischen Charakters nur aus Zweierzyklen bestehen, wird P_iP_{i+3} ein Zeichen x genau dann als Einerzyklus haben, wenn es ein Zeichen y gibt derart, daß sowohl P_i wie P_{i+3} das Paar $(x\ y)$ als Zweierzyklus haben. P_1 wie P_4 enthalten also den Zyklus (a s). Ein Satz der Gruppentheorie über echt involutorische Permutationen P_μ (bei geradem Alphabetumfang N) besagt nun, daß die Zyklen von P_iP_{i+3} in Paaren gleicher Länge auftreten:

Wenn P_i die Zweierzyklen $(x_1y_1), (x_2y_2), \ldots, (x_\mu y_\mu)$ enthält,
und P_{i+3} die Zweierzyklen $(y_1x_2), (y_2x_3), \ldots, (y_\mu x_1)$ enthält, dann
enthält P_iP_{i+3} die μ-Zyklen $(x_1x_2 \ldots x_\mu)$, $(y_\mu y_{\mu-1} \cdots y_1)$.

Schreibt man also einen der μ-Zyklen von P_iP_{i+3} in revertierter Reihenfolge ($\leftarrow$) an, so stehen die Paarungen zu Zweierzyklen von P_i und P_{i+3} direkt bzw. schräg übereinander:

$$\begin{array}{ll} \rightarrow & (\ x_1x_2 \ldots x_{\mu-1}x_\mu\ ) \\ \leftarrow & (\ y_1\, y_2 \cdots y_{\mu-1}\, y_\mu\ )\ . \end{array}$$

Wie nun die Zyklen aneinander zu heften sind, verbleibt als Frage.

19.6.2.2 Hier brachte *Rejewski* erstmals ein Häufigkeitsargument ins Spiel. Wenn man die Faulheit der Chiffrierer richtig einschätzt, dann müßte die fünfmal (nr 35. - nr 39.) auftretende identische Gruppe SYX SCW dem gängigsten Spruchschlüssel aaa entsprechen. Das legt in P_1 den Zweierzyklus (a s), in P_2 den Zweierzyklus (a y), in P_3 den Zweierzyklus (a x) fest, sowie in P_4 den Zweierzyklus (a s), in P_5 den Zweierzyklus (a c), in P_6 den Zweierzyklus (a w) . Damit steht für P_3 und P_6 bereits die Paarung der beiden Teilzyklen

↓
→ (a b v i k t j g f c q n y)
← (x l h e r z u d o m s p w)

fest; explizit kann man, mit (a x) beginnend, auch im Zickzack die Zweierzyklen ('swappings') von P_3 und P_6 ausrechnen:

---

[15] In den Jargon von *Bletchley Park* übernahm man den von dem polnischen Wortspiel *te same* („die selben") – *samiczka* („Weibchen") herrührenden Ausdruck '*female*'. Die meisten Leute in *Bletchley Park* kannten diesen Ursprung nicht und erklärten sich das Jargonwort anders, etwa mit *female screw* (Schraubenmutter).

P_3= (a x) (b l) (v h) (i e) (k r) (t z) (j u) (g d) (f o) (c m) (q s) (n p) (y w)

P_6= (x b) (l v) (h i) (e k) (r t) (z j) (u g) (d f) (o c) (m q) (s n) (p y) (w a)

P_3 enthält insbesondere auch den Zyklus (q s). Somit hat der Spruchschlüssel zu nr 1. AUQ AMN die Gestalt ∗∗s ; da P_1 den Zyklus (as) enthält, hat er sogar die Gestalt *s*∗s . Wenn man jetzt noch errät, daß der Spruchschlüssel zu nr 1. sss lautet, so ist in P_2 neben (a y) auch (s u) festgelegt. Damit steht auch die Paarung für die Teilzyklen von P_2 und P_5

→ ($\overset{\downarrow}{\text{a}}$ x t) (b l f q v e o $\overset{\downarrow}{\text{u}}$ m) (d)
← (y g c) (j n h r z i w s p) (k)

fest; es ergeben sich im Zickzack die Zweierzyklen von P_2 und P_5 :

P_2= (a y) (x g) (t c) (b j) (l n) (f h) (q r) (v z) (e i) (o w) (u s) (m p) (d k)

P_5= (y x) (g t) (c a) (j l) (n f) (h q) (r v) (z e) (i o) (w u) (s m) (p b) (k d)

Betrachtet man ferner noch die viermal (nr 30. - nr 33.) identisch auftretende Gruppe RJL WPX , so muß ihr Spruchschlüssel die Gestalt ∗bb haben. P_1 kann nur die Zweierzyklen (r b) oder (r c) haben; im ersteren Fall ergibt sich der wahrscheinlichere Spruchschlüssel bbb . Damit ist auch für die Festlegung von P_1 und P_4 die Paarung der Zweierzyklen (b r) bzw. (r c) bestimmt. Um auch die Zehnerzyklen richtig zu paaren, muß eine weitere Gruppe herangezogen werden, etwa (nr 19. - nr 20.) LDR HDE . Da P_3 und P_6 (r k) bzw. (k e) enthalten, sowie P_2 und P_5 (d k) bzw. (k d), muß der Spruchschlüssel die Gestalt ∗kk haben. Das legt die Stereotype kkk nahe, aus der sich ergibt, daß P_1 und P_4 die Zweierzyklen (l k) bzw. (k h) enthalten. Damit ist überdies die Paarung der Zehnerzyklen erledigt, es ergibt sich

→ (a) ($\overset{\downarrow}{\text{b}}$ c) (d v p f $\overset{\downarrow}{\text{k}}$ x g z y o)
← (s) (r w) (i e t h l q n u m j) und damit

P_1= (a s) (b r) (c w) (d i) (v e) (p t) (f h) (k l) (x q) (g n) (z u) (y m) (o j)

P_4= (s a) (r c) (w b) (i v) (e p) (t f) (h k) (l x) (q g) (n z) (u y) (m o) (j d)

Insgesamt erhält man also für die ersten drei Permutationen in geordneter Form

P_1 = (a s) (b r) (c w) (d i) (e v) (f h) (g n) (j o) (k l) (m y) (p t) (q x) (u z)

P_2 = (a y) (b j) (c t) (d k) (e i) (f h) (g x) (l n) (m p) (o w) (q r) (s u) (v z)

P_3 = (a x) (b l) (c m) (d g) (e i) (f o) (h v) (j u) (k r) (n p) (q s) (t z) (w y)

19.6.2.3 Die Entzifferung aller Spruchschlüssel ist damit auch geleistet (Abb. 151); die schlechten Angewohnheiten der ENIGMA-Chiffrierer führten nicht nur zu mehrfachem Gebrauch von identischen Spruchschlüsseln, sie werden besonders augenfällig, wenn man die Liste der Spruchschlüssel auf der Tastatur der ENIGMA (Abb. 152) betrachtet: Nur zwei von vierzig, nämlich abc und uvw , sind nicht völlig stereotyp, aber auch nicht sonderlich phantasievoll.

AUQ AMN : sss	IKG JKF : ddd	QGA LYB : xxx	VQZ PVR : ert
BNH CHL : rfv	IND JHU : dfg	RJL WPX : bbb	WTM RAO : ccc
BCT CGJ : rtz	JWF MIC : ooo	RFC WQQ : bnm	WKI RKK : cde
CIK BZT : wer	KHB XJV : lll	SYX SCW : aaa	XRS GNM : qqq
DDB VDV : ikl	LDR HDE : kkk	SJM SPO : abc	XOI GUK : qwe
EJP IPS : vbn	MAW UXP : yyy	SUG SMF : asd	XYW GCP : qay
FBR KLE : hjk	NXD QTU : ggg	TMN EBY : ppp	YPC OSQ : mmm
GPB ZSV : nml	NLU QFZ : ghj	TAA EXB : pyx	ZZY YRA : uvw
HNO THD : fff	OBU DLZ : jjj	USE NWH : zui	ZEF YOC : uio
HXV TTI : fgh	PVJ FEG : tzu	VII PZK : eee	ZSJ YWG : uuu

Abb. 151. Die 40 verschiedenen Spruchschlüssel entziffert

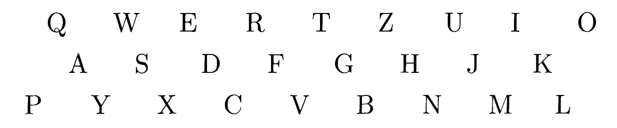


Abb. 152. Tastatur der ENIGMA

19.6.2.4 Im Januar 1933 gelang den jungen polnischen Mathematikern die erste Entzifferung deutscher Funksprüche. Das polnische Büro lernte sicher nicht viel aus dem semantischen Inhalt der Übungssprüche. Wichtiger war, daß nun die innere Verdrahtung der Rotoren aufgedeckt werden konnte. Da die Analyse auf sechs Zeichen am Anfang beschränkt war, wurde im wesentlichen nur der „schnelle" Rotor R_N (ganz rechts sitzend) bewegt, die übrigen ENIGMA-Rotoren blieben in 20 von 26 Fällen unbewegt. Das, zusammen mit ASCHEs Material, genügte *Jerzy Różycki* (1909–1942), um auch die innere Verdrahtung des jeweiligen Eingangsrotors zu rekonstruieren, und da die Rotorenlage damals alle Vierteljahre (ab 1936 monatlich, später täglich) wechselte, kam auch jeder Rotor in den Genuß der polnischen Untersuchung. Mit der Verfügbarkeit aller Spruchschlüssel ein und des selben Tages ließ sich der gesamte aufgefangene ENIGMA-Verkehr mit von den Polen nachgebauten Maschinen dechiffrieren.

19.6.2.5 Um auch die Grundstellung des Tagesschlüssels zu rekonstruieren, machten sich die Polen zunutze, daß die Zyklenlängen in den drei $P_i P_{i+3}$ von der Wahl der Steckerverbindung T unabhängig sind. Den geläufigen Satz aus der Theorie der Permutationsgruppen (vgl. 7.2.4)

S und TST^{-1} haben übereinstimmende Zyklenstruktur ('*characteristic*')

hat *Deavours* plakativ *the theorem that won World War II* genannt. Die Anzahl verschiedener Zyklenaufteilungen ist wegen der Paarigkeit gleich der Anzahl der Partitionen von 13 und beträgt 101; für die $6 \times 26 \times 26 \times 26 \approx 10^5$ Grundstellungen reichen drei solche Partitionen – im obigen Beispiel sind es die **Charakteristiken** 10+2+1, 9+3+1, 13 – im allgemeinen zur eindeutigen Charakterisierung aus. *Rejewski*, unterstützt von *Różycki* und *Zygalski*,

stellte mit Hilfe der rekonstruierten ENIGMAs nun einen Katalog auf, der zu allen Grundstellungen die Partition der Zyklen enthielt. Wichtig war, daß diese Untersuchung *von der gewählten Steckerverbindung unabhängig* war. Um sie zu mechanisieren, wurde in der Fabrik AVA in der Stepinska-Straße ein ‚Zyklometer' genanntes Gerät gebaut. Das *Biuro Szyfrów* hatte 1937 den Katalog fertig; die Tagesschlüssel waren damit in 10 bis 20 Minuten zu lösen.[16]

19.6.2.6 Als Problem verblieb, die Ringstellung herauszufinden. Das exhaustive Vorgehen konnte wesentlich erleichtert werden durch eine Beobachtung, die *Rejewski* schon 1932, dank des Materials von ASCHE, gemacht hatte: daß die meisten Klartexte mit /anx/ begannen – wobei /x/ als Ersatz für Zwischenraum diente. Nach *Kerckhoffs*' Maxime mußte man damit rechnen, daß die Maschine kompromittiert war; um so unvernünftiger war es, einen stereotypen Anfang zuzulassen. Dieser triviale Fall einer Klartext-Geheimtext-Kompromittierung (vgl. 14.4) wird in 19.7 wieder aufgegriffen werden.

19.6.3 Polen II . All diese Erfolge waren nur möglich dank des *echt* involutorischen Charakters der Rotorchiffrierung der ENIGMA; die Umkehrwalze von *Scherbius* und *Korn* erwies sich als grandiose *complication illusoire*. Die Chiffriermaschinen von *Boris Hagelin* litten nicht unter *diesem* Mangel. Aber auch die in Amerika nachgebaute M-209 wurde von den Deutschen ab 1942 in Nordafrika gebrochen.

19.6.3.1 1938 verschärfte sich die Situation. Die Deutschen änderten nämlich am 15. September 1938 die Chiffriervorschrift und führten am 15. Dezember 1938 einen vierten und einen fünften Chiffrierrotor ein, was zu sechzig möglichen Rotorenlagen, statt bisher sechs, führte.

Mit der letzteren Komplikation wurden die Polen rasch fertig, denn es kam ihnen ein glücklicher Zufall zu Hilfe. Der SD (‚Sicherheitsdienst') hatte den Einfall, seine Funksprüche erst mit einem einfachen Verfahren von Hand zu chiffrieren, bevor sie mit der ENIGMA chiffriert wurden – man wollte sich offenbar von den ENIGMA-Chiffrierern nicht in die Karten schauen lassen. Die Polen konnten die ENIGMA-Chiffrierung zwar abstreifen, erzielten aber damit einen ‚sinnlosen' Text. Sie dachten zunächst an das nächstliegendste, daß der SD ein besonderes, ein anderes Chiffrierverfahren verwende. Als aber 1937 eines Tages in dem Gestammel das klar lesbare Wort /eins/ auftauchte, erkannte man den wahren Sachverhalt: Der ENIGMA-Chiffrierer hatte einen Text bekommen, der versehentlich die Ziffer 1 enthielt und hatte diese – was sollte er sonst tun – als Klartext /eins/ eingegeben. Die einfache Chiffrierung des SD konnte B.S.-4 unschwer abstreifen und somit Sprüche des SD lesen. Der SD änderte nun im September 1938 die Chiffriervorschrift

[16] Die Polen hatten vorher auch die ‚Raster-Methode' (*metoda rusztu*, engl. *grill method*, *grid method*, *grate method*) benutzt. Sie war '*manual and tedious*' (*Rejewski*) und nur brauchbar, solange wenige Steckerverbindungen (bis 1. 10. 1936 deren sechs) benutzt wurden. Man konnte damit die Ringstellung des „schnellen" Rotors herausfinden. Details wurden 1979, 1980 von *Józef Garliński* und 1980, 1981 von *Marian Rejewski* publiziert.

nicht, führte aber im Dezember 1938 den vierten und fünften Rotor ein. Damit kamen auch diese Rotoren unter Beobachtung und nach kurzem waren ihre inneren Verbindungen aufgedeckt. Das Nebeneinander zweier zweier Chiffrierverfahren, von denen das eine als kompromittiert zu gelten hatte, war ein schwerer Fehler.

19.6.3.2 Es verblieb, mit der neuen Chiffriervorschrift, die bis Ende April 1940 galt, zurechtzukommen. Diese benutzte nicht mehr die selbe Grundstellung für den ganzen Tag, sondern der Chiffrierer sollte willkürlich für jeden Spruch seine eigene wählen. Diese wurde *unchiffriert* dem Funkspruch vorangestellt, sodann folgte der (immer noch verdoppelte[17]) Spruchschlüssel (*plain indicator*), chiffriert mit dieser individuellen Grundstellung. Beginnt also ein Spruch mit RTJWA HWIK..... , so ist rtj die Grundstellung, WAH WIK ist der mit dieser Grundstellung chiffrierte Spruchschlüssel, wofür wir im folgenden rtj | WAH WIK schreiben werden. Mit der Grundstellung rtj ermittelt der Dechiffrierer aus WAH WIK den verdoppelten Spruchschlüssel (von dem also feststeht, daß er das Muster *123123* haben muß); mit der ersten Hälfte des dechiffrierten Spruchschlüssels (dem *plain indicator*) als Grundstellung dechiffriert er den restlichen Spruch.

Da die Ringstellung und die Rotorenlage unbekannt waren, konnte der Gegner mit der vorangestellten Grundstellung unmittelbar nichts anfangen: Der Suchraum enthielt noch 1 054 560 Fälle (26^3 Ringstellungen, 6 Rotorenlagen, ab Dezember 1938 10 Auswahlen von 3 Rotoren aus 5).

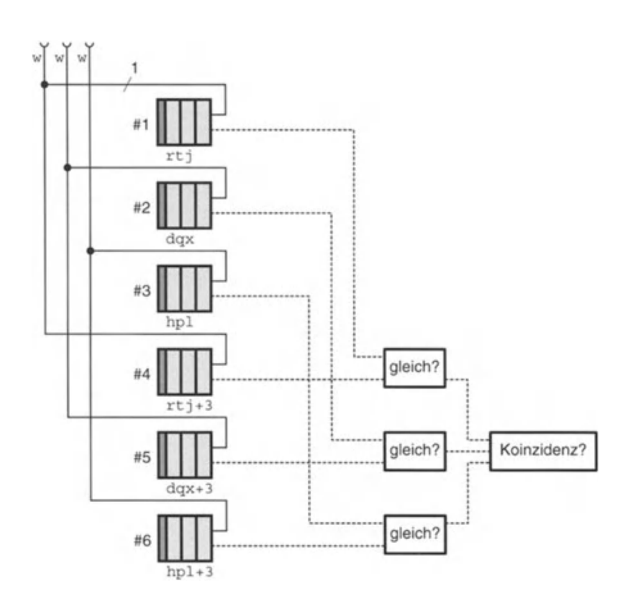


Abb. 153. Funktionsweise einer polnischen *bomba* (Herbst 1938)

[17] Die Chiffrierung des verdoppelten Spruchschlüssels wurde nach *Peter Twinn* für die 4-Rotor Abwehr-ENIGMA bis Ende des Krieges beibehalten.

19.6.3.3 Immerhin war das ein Fall für eine Mustersuche, und zwar nach dem Muster *123123* – noch galt ja die Spruchschlüsselverdopplung. Eine Mechanisierung dieser sehr mühevollen Arbeit lag nahe. *Rejewski* ließ noch im Oktober 1938 bei AVA sechs Maschinen bauen, die die sechs Rotorenlagen simulierten, und spielte auf jeder die 17 576 Ringstellungen durch, wozu man maximal 110 Minuten brauchte. Die ‚richtige' Ringstellung fand man unter Benutzung der Einerzyklen folgendermaßen: Man baute die Maschine aus drei Paaren von ENIGMA-Rotorensätzen auf; in jedem Paar waren die Stellungen der Rotorensätze um drei Positionen versetzt, die Stellung der Rotorensätze des ersten Paars war gegen die des zweiten Paares um eine Position versetzt und die des zweiten Paares gegen die des dritten Paares ebenfalls um eine Position. Sobald genügend Material vorlag, um über drei chiffrierte verdoppelte Spruchschlüssel zu verfügen, von denen der erste an der ersten und vierten Stelle, der zweite an der zweiten und fünften Stelle, der dritte an der dritten und sechsten Stelle ein und den selben Buchstaben – etwa den Buchstaben W in

rtj	WAH WIK
dqx	DWJ MWR
hpl	RAW KTW

und damit nach 19.6.2.1 einen Einerzyklus (‚Fixpunkt') aufzeigte – war ein erfolgversprechender Angriff (Abb. 153) möglich: Man startete nun die Maschine mit den drei Voreinstellungen rtj, dqx und hpl , wiederholte ständig die Eingabe des **Testbuchstabens** W und hatte nur abzuwarten, bis sich in jedem der drei Paare jeweils ein gleicher Buchstabe einstellte, also das Muster *123123* gefunden war. Eine solche Koinzidenz führte über eine einfache Relais-Schaltung zum Anhalten der ganzen Apparatur, die die Polen wegen ihres Aussehens *bomba* nannten.[18] Gelegentlich gab es auch falschen Alarm.

Die *bomba* war gegen Steckerverbindungen empfindlich; die Methode funktionierte nur, wenn der Testbuchstabe (im obigen Beispiel W) „ungesteckert" war. Die Wahrscheinlichkeit dafür lag bei Verwendung von fünf bis acht Steckern bei 50% . (Hätte man dagegen drei verschiedene Fixpunkte verwendet, wie es die Briten ursprünglich vorsahen, wäre die Wahrscheinlichkeit auf 12.5% zurückgegangen.)

Nach dieser Ermittlung der Ringstellung konnte man durch Vergleich der chiffrierten verdoppelten Spruchschlüssel mit den auf der ENIGMA-Replik (mit den ermittelten Ringstellungen) angezeigten Chiffrierungen auch die Steckerverbindung rekonstruieren. Damit waren alle Sprüche des betreffenden Tages (später der betreffenden Acht-Stunden-Schicht) aus dem jeweiligen ‚Netz' (es gab im Krieg bis zu 120 solche Netze) bloßgestellt.

19.6.3.4 Eine andere Art der Mechanisierung entwickelte im Herbst 1938 *Henryk Zygalski* (1907–1978): Ein Lochblattverfahren ('card catalog') zur Ermittlung der Tagesschlüssel aus etwa zehn bis zwölf (beliebigen) Fixpunkten.

---

[18] Nach *Lisicki* ursprünglich Bezeichnung für eine Eistorte („Eis-Bombe").

$\langle R_N \rangle$																											
z	o	o		o	o	o		o	o	o	o	o	o	o					o			o	o	o		o	
y				o	o				o	o	o			o			o	o			o	o					
x	o	o	o		o	o	o	o	o		o	o	o		o				o		o	o	o				
w	o	o	o					o	o	o				o				o	o		o	o	o		o		
v	o		o	o	o	o						o							o	o		o		o	o		
u		o		o			o	o				o		o			o	o				o	o	o	o	o	
t	o				o	o							o				o				o	o	o	o	o	o	
s	o							o		o	o	o											o	o	o		
r	o	o	o		o	o	o			o			o	o			o			o	o	o			o	o	
q										o		o	o	o	o		o	o	o					o		o	
p		o	o	o		o		o	o	o					o		o	o					o				
o	o		o				o	o	o	o					o			o	o	o	o			o			
n		o		o	o		o	o			o			o						o			o	o			
m		o	o	o			o	o		o	o			o	o		o			o	o	o					
l		o		o							o	o	o					o	o	o			o		o		
k	o						o		o	o				o					o		o	o	o		o	o	
j	o	o		o		o					o	o	o				o		o		o	o	o		o		
i		o	o				o	o			o	o	o		o	o	o	o			o	o	o	o	o	o	
h	o	o	o		o	o	o	o		o	o	o			o		o				o		o				
g	o	o	o	o	o	o	o	o	o					o			o	o	o					o	o	o	
f			o	o		o			o	o	o	o	o	o	o		o			o		o	o	o	o	o	
e				o			o			o		o		o			o				o			o		o	
d			o		o	o				o	o		o	o						o	o	o			o		
c	o	o	o		o		o			o	o	o	o		o	o	o	o	o			o		o	o		
b			o			o	o		o		o	o	o	o	o	o	o		o		o	o			o		
a	o	o		o				o	o	o	o	o	o	o	o		o	o	o						o		
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	$\langle R_M \rangle$

Abb. 154. Zygalski-Lochblatt K_{14}^{413} für Rotorenlage IV-I-III, Lochungen zeigen mögliche Fixpunkte (Einerzyklen) von P_1P_4 für Grundstellung $\langle R_L\rangle\langle R_M\rangle\langle R_N\rangle$, $\langle R_L\rangle$=k.

Für 6 Rotorenlagen wurde bezüglich P_1P_4, P_2P_5 oder P_3P_6 festgestellt, ob für eine Grundstellung $\langle R_L\rangle\langle R_M\rangle\langle R_N\rangle$ von R_L, R_M, R_N irgendein Einerzyklus überhaupt möglich ist. Für jeden der 26 Buchstaben $\langle R_L\rangle$ wurde dies in einer $\langle R_M\rangle \times \langle R_N\rangle$-Matrix durch eine Lochung ('*female*') festgehalten (Abb. 154); grob gerechnet traten 40% Löcher auf. Durch Übereinanderlegen der jeweiligen, entsprechend der Grundstellung $\langle R_M\rangle\langle R_N\rangle$ verschobenen Blätter[19] wurde die mögliche Ringstellung bestimmt; in der Regel eindeutig, sobald ungefähr zehn bis zwölf Fixpunkte verfügbar waren. Das Verfahren war unabhängig von der Steckerverbindung und war damit auch noch brauchbar, als (ab 19.8.1939) zehn Stecker benutzt wurden — so lange jedenfalls, als die Spruchschlüsselwiederholung anhielt. Es ist eine Ironie, daß die Deutschen, die stets versucht hatten, durch geeignete Vorschriften zur Chiffriersicherheit eine *Kerckhoffs*sche Superimposition unmöglich zu machen, nun Opfer einer Kette von Vorgehensweisen wurden, die (19.6.1) durch eine banale Schwachstelle eingeleitet wurde.

[19] Tatsächlich wurden, um volle Überdeckung zu ermöglichen, Blätter von 51×51 Feldern, die durch waagrechte und senkrechte Duplikation entstanden, benutzt.

19.6.4 Großbritannien. Schon am 9. Januar 1939, bei einem Besuch in Paris, hatte der polnische Oberstleutnant *Karol Gwido Langer* (1884–1951) seine französischen Kontakte durch Fühlungnahme mit seinen britischen Kollegen abgerundet. Mit steigender Kriegsgefahr war weitere Zusammenarbeit angezeigt. An einem Treffen am 25. Juli 1939 in Warschau nahmen neben *Dilly Knox*, dem führenden britischen Kryptanalysten im Foreign Office, seinem Chef *Alastair Denniston*[20], dem Leiter der *Government Code and Cypher School* (GC&CS) und dem geheimnisvollen Cdr. Humphrey Sandwith ('Mr. Sandwich') auch Commandant *Bertrand* und Capitaine *Braquenié* teil. Die Polen, mit Major *Ciężki, Langer*, dem Grand Chef Oberst *Stefan Mayer* und den jungen mathematischen Mitarbeitern *Rejewski*, *Zygalski*, *Różycki* zeigten ihnen in Pyry, im Süden Warschaus, stolz alle ihre Ergebnisse. Bei diesem Treffen bekamen sowohl die Franzosen wie die Briten auch polnische Repliken der ENIGMA mit allen fünf Rotoren. Die Gäste waren überwältigt.

Die Briten hatten seit der Krise, die zum Münchner Abkommen vom Herbst 1938 führte, eine Ausweichmöglichkeit ihres unter der Adresse 56 Broadway (Whitehall), Westminster geführten, als '*Room 47*' des *Foreign Office* bekannten Dienstes ins Auge gefaßt, und zwar in *Bletchley Park* (kurz BP, Deckname 'Station X'), rund 80 km nördlich von London. Seit dem Beginn der zum Krieg führenden Spannungen dort fest angesiedelt, benutzten die Briten nun ab Anfang Januar 1940 die polnischen Lochblattverfahren; die Lochblätter nannten sie '*canvasses*' oder nach *John Jeffreys*, der ihre Herstellung zu überwachen hatte, '*Jeffreys sheets*'. Für die polnische *bomba* – die Briten sprachen später ebenfalls von '*bomb*' – war jedoch eine Weiterentwicklung angezeigt, um sechzig statt sechs Rotorlagen durchzuspielen.

Oliver Strachey[21] hatte den jungen *Alan Mathison Turing*, der sich bereits als Logiker einen Namen gemacht hatte, der aber von Kindheit an an Chiffrierung interessiert war, mehrfach in Kontakt mit *Alfred Dillwyn Knox*[22] gebracht, einem Altphilologen, der schon 1915 den '*Room 40*' der *Royal Navy* dem Fellow des Kings College in Cambridge vorgezogen hatte und der sich bisher erfolgreich nur mit der kommerziellen ENIGMA ohne Steckerbrett, die die Italiener und Spanier benutzten, herumgeschlagen hatte (14.5).

Mit Kriegsbeginn begann *Turing* dort seine Arbeit. Unter ihm und etwas später dem Mathematiker *Gordon Welchman* (1906–1985) wurden die polnischen Bomben weiterentwickelt, wobei *Turing* auf seine Erfahrungen mit Relaisschaltungen – er hatte (5.7.3) in Princeton 1937 einen Relais-Multiplizierer entworfen und prototypisch gebaut – zurückgreifen konnte. *Turing* war nicht nur von Kindheit an und inzwischen auch theoretisch an der Kryptologie interessiert; er hatte auch schon Kontakte zur *Government Code and Cypher*

[20] *Denniston* wurde Mitte 1940 abgelöst, sein Nachfolger wurde *Edward Travis*.

[21] *Oliver Strachey*, Ehemann der Feministin *Ray Strachey* und Vater des Informatikers *Christopher Strachey*, ersetzte 1941 in kanadischen Diensten den ehemaligen U.S. Major *Herbert Osborne Yardley*, der in den Vereinigten Staaten in Ungnade gefallen war.

[22] *Knox* erlag am 27. Februar 1943 einem Krebsleiden.

School, möglicherweise bis 1936 zurückreichend, und hatte im Sommer und um Weihnachten 1938 – *Denniston* sorgte vor – dort Kurse besucht.

Im Januar 1940 brach *Bletchley Park* unter Verwendung von Zygalski-Lochblättern erstmals ENIGMA-Schlüssel, darunter die Tagesschlüssel vom 6. und 17. Januar der achtlos funkenden Luftwaffe. Das Schlüsselnetz, in das sie einbrachen, nannten die Briten RED. Das war der Anfang.

19.6.4.1 Als *Turing* Mitte Januar 1940 den nach Frankreich geflüchteten *Rejewski* in Gretz-Armainvilliers, südöstlich von Paris von Paris, traf, war er, *Rejewski* zufolge, sehr interessiert an den polnischen Erkenntnissen über die Behandlung der Steckerverbindungen. Er erzählte den Polen jedoch nicht, wie weit er schon gekommen war (s. 19.7). Es lag nahe, daß *Turing* bestrebt war, die polnische *bomba* wie die Zygalski-Blätter gegen Steckerverbindungen unempfindlich zu machen, da die Deutschen Schritt für Schritt weniger „ungesteckerte“ Buchstaben verwendeten..

Die Polen waren bei der *bomba* im wesentlichen dem elektrischen Aufbau der ENIGMA gefolgt, der über den Umkehrrotor einen hin- und zurücklaufenden Strompfad vorsah. Solange nur jeweils eine Alphabettaste gedrückt wurde und nur eine Lampe aufleuchten sollte, war diese Idee recht praktisch. Turing wollte sich jedoch im Herbst 1939 vor allem von der Einengung auf die wenigen verbliebenen „ungesteckerten“ Testbuchstaben frei machen. Durch eine 26-adrige Verbindung sollte, wie Joan Murray née Clarke (1917–1996) sich erinnert, ein schnelleres und zielstrebigeres, paralleles *'simultaneous scanning'* aller 26 Möglichkeiten des Testbuchstabens erreicht werden. Turing ersetzte also die Rotor-Reflektor-Anordnung durch einen **Vertauscher** (*Welchman*: *'double-ended scrambler'*, U.S. Jargon *'commutator'*, *'straight-through rotor'*) aus sechs Rotoren, der eine 26-adrige Eingangsseite und eine 26-adrige Ausgangsseite hatte, im übrigen aber die klassische ENIGMA-Substitution $P_i = S_i U S_i^{-1}$ nachbildete, die der i-ten Stellung der drei Rotoren der Anordnung entsprach, dem i-ten von insgesamt 26^3 Zuständen. Dabei war, wegen des involutorischen Charakters der ENIGMA-Substitution, ein solcher Vertauscher symmetrisch bezüglich Eingangs- und Ausgangsseite aufgebaut.

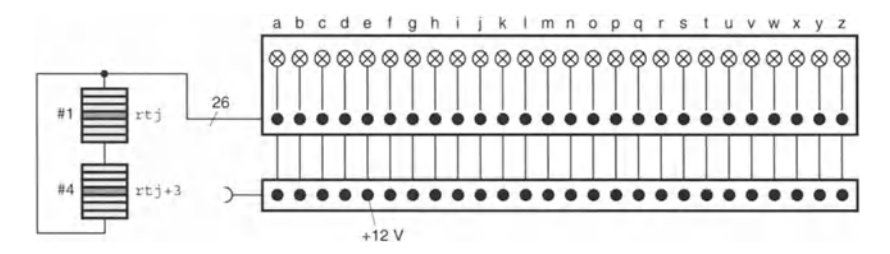


Abb. 155. Hypothetische Turing-Version einer polnischen *bomba* (mit *'simultaneous scanning'*) – Schaltung einer der drei Schleifen

Die polnische *bomba* lief in dieser *Turing*schen Version einer BOMBE auf drei geschlossene Schleifen von je zwei Vertauschern hinaus, von denen Abb. 155 eine zeigt. *Turing* war es damit gelungen, die Überchiffrierung durch die

Steckerbrettsubstitution maschinell abzustreifen: Er erkannte, daß die Einerzyklen, die besagten *females* der Zygalski-Blätter, die natürlich Fixpunkte einer Abbildung waren, auch durch einen rückgekoppelten Iterationsprozeß bestimmt waren, der normalerweise divergierte und damit anzeigte, daß die betreffende Rotorenstellung keinen Fixpunkt erlaubte; wenn er nicht divergierte, lieferte er Fixpunkte. Der Logiker *Turing*, dem der Gebrauch der doppelten Verneinung (‚reductio ad absurdum') geläufig war, wandte sich damit dem allgemeineren Prinzip der Rückkopplung zu.

Technisch geschah die Unterscheidung der beiden Fälle durch ein **Testregister**, das an die 26-adrigen Verbindungsleitungen der Rückkopplung (von #4 nach #1) angeschlossen war; die zum Testbuchstaben (W in unserem Beispiel) gehörige Leitung wurde unter Spannung gesetzt. Im Divergenzfall leuchteten alle Lampen des Testregisters auf. Im Fall eines Fixpunktes war die zugehörige Rückkopplungsschleife galvanisch getrennt vom Rest der Zusammenschaltung; dementsprechend leuchtete genau eine Lampe (die zu W gehörige), wenn die Steckerverbindung getroffen war, andernfalls alle Lampen bis auf eine.

Eine Batterie von Vertauschern sollte simultan fortgeschaltet werden können. *Turing* wäre damit auch in der Lage gewesen, durch geeignete Zusammenschaltung von Vertauschern die Wirkungsweise der polnischen *bomba* nachzubilden. Die Entwicklung verlief jedoch anders, nämlich allgemeiner (19.7).

Bereits im letzten Vierteljahr 1939 bekam *Bletchley Park* die Genehmigung, von der *British Tabulating Machine Company* in Letchworth eine BOMBE zum Brechen der ENIGMA bauen zu lassen. Die Leitung übernahm *Harold 'Doc' Keen* mit einer Mannschaft von zwölf Leuten. Die Turing-BOMBE entstand in erstaunlich kurzer Zeit, sie war im Frühjahr 1940 einsatzbereit.

Welchman kam übrigens im Herbst 1939, als er sich noch in der Schulung befand, unabhängig zu ähnlichen Gedankengängen, obwohl er zunächst mit der maschinellen ENIGMA-Entzifferung nicht betraut war. Er erfand dabei auch die Lochblätter von *Zygalski* wieder – nicht wissend, daß *John Jeffreys* in einem anderen Gebäude schon an ihrer Herstellung arbeitete. Ebensowenig wußte er zunächst von *Turing*s Absichten – er brauchte das auch nicht zu wissen.

19.6.4.2 *Turing* hat möglicherweise bereits vor dem Treffen in *Pyry* daran gedacht, wahrscheinliche Wörter zum Brechen der ENIGMA heranzuziehen. Nach diesem Treffen, das ihm die polnische *bomba* offenbarte, wandte er wohl seine Gedanken verstärkt der Mechanisierung *seiner* Methode zu. Der Hauptvorteil der Turing-BOMBE war, daß sie nicht nur, wie die Zygalski-Blätter, die Rotorenlage fand, sondern auch mindestens eine Steckerverbindung.

Die Briten waren jedenfalls Anfang 1940 so tief in die Details der ENIGMA und der Gewohnheiten der Deutschen eingedrungen, daß sie auch auf den erwarteten nächsten Schlag vorbereitet waren: Als nämlich am 1. Mai 1940, kurz vor dem Beginn des Feldzugs in Frankreich, die Deutschen bei Heer

und Luftwaffe von der Verdoppelung des Spruchschlüssels abgingen[23] und damit die bisherigen Methoden – nicht nur die polnischen Bomben, sondern auch die Zygalski-Jeffreys-Blätter – wertlos wurden. Da inzwischen das System offen lag, konnte man hoffen, die gewünschten Rückkopplungen mittels Klartext-Geheimtext-Kompromittierung zu bekommen – die Vorliebe der Deutschen für stereotype Wendungen wie /wettervorhersage biskaya/, /wettervorhersage deutsche bucht/ etc., oder /obersturmbannführer/, obergruppenführer/ etc., oder /keine besonderen ereignisse/ war nur zu gut bekannt. Der Prototyp 'Victory' der Turing-BOMBE wurde am 18. März 1940 installiert. Ab 8. August 1940 folgten die ersten regulären *spider*: 'Agnes', 'Jumbo', 'Funf', ... ; 'Ming' war am 26. Mai 1941 fertig. Mehr darüber in 19.7.

"It was he [*Turing*] who first formulated the principle of mechanizing a search for logical consistency based on a 'probable word' " (*Andrew Hodges*). *Turing* hatte überdies die britische BOMBE in einer Weise entworfen, die ein universelles Arbeiten ermöglichte.

19.6.4.3 Wenn aber die Suche mittels wahrscheinlicher Wörter vergeblich blieb, bestand immer noch die Möglichkeit einer phasenrichtigen Superimposition (19.3). Dazu wurden Parallelstellen gesucht; die verwendete Methode wurde *'banburism'* genannt, weil die dazu benutzten 1-aus-26-Lochblätter in Banbury, einer Kleinstadt nahe Oxford, hergestellt wurden. *Turing* entwickelte dazu eine Bewertung der Parallelstellen ('*weight of evidence*') in einer logarithmischen Einheit [ban], die ein dezimales Gegenstück zur binären Informationseinheit [bit] von *Claude Shannon* war, 1 [ban] $\hat{=}$ ${}^2\log 10$ [bit]. 1 [deciban] $\approx$ 0.332 [bit] war in *Bletchley Park* eine praktische Einheit.

Turing und *Shannon* waren in ihren Vorgehensweisen voneinander unabhängig, die beiden trafen sich erst gegen Ende 1942. "Turing and I never talked about cryptography" (Claude Shannon). Es könnte sehr wohl sein, daß man in Bletchley Park bis Juli 1941 den Kappa-Test nach *Friedman* (17.1) oder den Phi-Test nach *Kullback* (17.5) nicht kannte; wie *Turing* seine '*repetition frequency*' (in seinem *Treatise on the Enigma*, geschrieben im Spätsommer oder Frühherbst 1940) fand, ist bisher unklar geblieben.

'banburism' war eine Vervollkommnung der Methode, die schon die Polen benutzt hatten (‚Uhrzeigermethode' von *Jerzy Różycki*[24]). Die Ausrichtung ('*alignment*') der Chiffrate ergab die Differenz der Phasenlagen der unchiffrierten Spruchschlüssel. Damit war wenigstens der jeweilige schnelle Rotor R_N (dessen Grundstellung durch die dritte Stelle des Spruchschlüssels bezeichnet wird) zu bestimmen, was die Arbeit mit den Bomben sehr vereinfachte. *Deavours* und *Kruh* geben dazu folgendes Beispiel: Aus etlichen phasenrichtig ausgerichteten Paaren von aufgefangenen Sprüchen ergaben sich für die 3. Stelle des *chiffrierten* Spruchschlüssels folgende beobachtete Werte:

[23] Die Kriegsmarine verwendete keine Verdopplung, sondern überchiffrierte einen völlig frei gewählten Spruchschlüssel und eine je nach dem Schlüsselnetz aus einer Liste auszuwählende Kenngruppe mit einer Bigrammsubstitution (4.1.2).

[24] Różycki kam am 9. Januar 1942 beim Untergang des Schiffes *Lamoricière* ums Leben.

erster Spruch	R	F	D	T	N	M	K	B	M	N
zweiter Spruch	F	K	Y	Y	Q	Q	O	Y	C	K
Differenz der Phasenlage *mod.* 26	07	12	04	02	14	21	06	11	06	03

Diese Daten schließen sich zu zwei Ketten mit Ausgangslagen für R und D:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
R				Q			F		M						C	N			K						O
D		T		Y															B						

Fährt man an der ersten Kette mit dem Klartextalphabet entlang, so kommt eine Involution, nämlich (k n) zustande für folgende Lage:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	F		M						C	N			K						O	R				Q	

Alle Möglichkeiten für Involutionen ausnützend, erhält man die Hülle

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	F	J	M	B					C	N		D	K	T		Y	U		O	R				Q	

die mit der zweiten Kette in geeigneter Lage, nämlich

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
				B								D		T		Y									

verträglich ist. Damit sind vierzehn Anfangsstellungen des schnellen Rotors aufgeklärt. Für die Rotoren I bis V konnte so die Lage der Nut (8.5.3) festgestellt werden und damit, welcher Rotor als „schneller“ Rotor eingesetzt war. Damit konnte in der polnischen *bomba* und der britischen BOMBE die Anzahl der durchzuspielenden Rotorlagen stark reduziert werden.

19.6.5 Frankreich II . Rejewski, Zygalski und Różycki konnten beim Zusammenbruch Polens nach Rumänien flüchten, sie wurden von den Franzosen ‚gerettet‘ und nach Frankreich gebracht, wo sie Ende September 1939 unter Commandant *Bertrand* im *Château de Vignolles* bei Gretz-Armainvilliers (Deckname ‘*Poste de Commandement* Bruno’), 50 km südöstlich von Paris, die französischen Dechiffrierer verstärkten. Bis zum deutschen Angriff auf Frankreich im Mai 1940 wurden dort mittels Zygalski-Lochblättern, die aus Bletchley Park geliefert wurden, von der ‚Gruppe Z‘ fast gleichviel ENIGMA-Funksprüche gebrochen wie in BP, hauptsächlich Heeresverwaltung (GREEN, erstmals um den 17.1.1940 der Tagesschlüssel vom 28.10.1939) und Luftwaffe (RED, erstmals um den 25.1.1940 der Tagesschlüssel vom 6.1.1940), sowie nach der Invasion Norwegens die des Fliegerführer Trondheim (YELLOW).

Nach dem Zusammenbruch Frankreichs (‚Fall Gelb‘) wurde P.C. Bruno zunächst am 24. Juni 1940 nach Oran in Algerien verlegt, im Oktober 1940 aber zurückverlegt nach dem *Château des Fouzes* bei Uzès (Deckname ‘*Cadix*’) im unbesetzten Teil Frankreichs. Da die Zygalski-Blätter seit 1. Mai 1940 nutzlos geworden waren, mußten sich Polen wie Briten zunächst mit *Cillis* und *Herivel tips* (19.7) durchschlagen. Die von den Briten ‘Expositur 3000‘ genannte, vom polnischen Oberstleutnant Langer geführte Einheit mußte am 9. November 1942, nach der Landung der Alliierten in Nordafrika, flüchten. Rejewski und Zygalski erreichten nach einigen Umwegen über Gibraltar am 3. August 1943 London, wo sie weiter kryptanalytisch arbeiteten — Bletchley Park mit den Turing-Bomben und den Colossi blieb ihnen jedoch verschlossen.

19.7 Klartext-Geheimtext-Kompromittierung: Rückkoppelpläne

Das ENIGMA-System war für die Briten im Mai 1940 praktisch offengelegt. Die Idee der Rückkopplung, die man dank *Turing* (und *Welchman*) seit Ende 1939 verfolgte, und die Geräte, die man ab Frühherbst 1940 in *Bletchley Park* verfügbar hatte, waren, wie gesagt, zu dem Zweck geeignet, auf wahrscheinliche Wörter zu prüfen, also eine Klartext-Geheimtext-Kompromittierung aufzusuchen. Damit wurde methodisch der Ansatz wieder aufgenommen, den schon 1932 *Rejewski* (vgl. 19.6.2.4) benutzt hatte. Systematisch gehörte deshalb der folgende Abschnitt eigentlich an den Schluß des Kapitels 14.

Die Briten sahen die Notwendigkeit vor sich, täglich das Menü für die Suche mit Hilfe geeigneter *'cribs'* von wahrscheinlichen Wörtern zu bereiten. Unterstützt wurden sie zwischenzeitlich durch fortgesetzte Verstöße auf deutscher Seite gegen die einfachsten Regeln der Chiffriersicherheit. *John Herivel* fiel im Mai 1940 auf, daß beim Schlüsselwechsel die neue Grundstellung häufig nahe an der vorher eingestellten Ringstellung lag oder gar mit ihr übereinstimmte ('*Herivel tip*') – eine Folge schlampiger Hantierung. Außerdem hielt der Gebrauch stereotyper Spruchschlüssel an – die Briten reihten sie unter der Rubrik *'Cillis'* ein.[25] Wiederum war der Schaden bereits angerichtet, als es der deutschen Überwachung allmählich gelang, die Chiffrierfehler einzudämmen. Übrigens war die Luftwaffe des verblendeten, großsprecherischen Emporkömmlings *Hermann Göring* am nachlässigsten in der Chiffriersicherheit. Die Mathematiker und Philologen von *Bletchley Park* konnten schon ab 26. Mai 1940, bevor die BOMBE benutzbar war, regelmäßig den ENIGMA-Verkehr der Luftwaffe (Schlüsselnetz RED) brechen, während sie mit den Sprüchen der Kriegsmarine Schlüsselnetz DOLPHIN „Heimische Gewässer“, später „Hydra“) erst ab Juni 1941 einigermaßen zurechtkamen. Im Dezember 1940 gelang auch der Einbruch in den Funkverkehr der SS (Schlüsselnetz ORANGE), ab September 1941 war *Rommel*s ENIGMA-Verbindung mit Berlin gebrochen. Ab 1942 erzielten die Briten tiefe und anhaltende Einbrüche, vor allem bei der heftig funkenden Luftwaffe (Schlüsselnetze WASP des Fliegerkorps IX, GADFLY des Fliegerkorps X, HORNET des Fliegerkorps IV, SCORPION des Fliegerführer Afrika). Am widerspenstigsten erwies sich nach britischen Angaben der von gut ausgebildeten Leuten diszipliniert geführte Funkverkehr innerhalb des Heeres: Vor Frühjahr 1942 wurde keine einzige ENIGMA-Verbindung des Heeres (außer einer in Rußland, Schlüsselnetz VULTURE I) bloßgestellt.

19.7.1 *Turing* und parallel *Welchman* verwendeten statt der drei isolierten, zweigliedrigen Zyklen der polnischen *bomba* ein ganzes System von rückgekoppelten Maschen, gebildet aus zunächst 10, später 12 Vertauschern. Ihre

[25] Gelegentlich als *'sillies'* interpretiert. Welchkman: 'I have no idea how the term arose'. Hierunter fällt auch der Fehler, als Spruchschlüssel die Grundstellung zu wählen, von den Briten (*Dennis Babbage*) JABJAB genannt.

Technik der **Rückkoppelpläne** für die Vertauscher erinnert den Informatiker heute sehr an Übergangsdiagramme der Automatentheorie. Folgendes Beispiel[26] geht im Kern auf *Cipher A. Devours* und *Louis Kruh* zurück.

Als wahrscheinliches Wort sei /oberkommandoderwehrmacht/ vermutet. Es soll gegen den Geheimtext

OVRLJ BZMGE RFEWM LKMTA WXTSW VUINZ GYOLY FMKMS GOFTU EIU...

geprüft werden. Nach 14.1 kann nicht jede Lage vorkommen, da kein Zeichen durch das selbe Zeichen chiffriert werden kann. Von den nicht allzuvielen verbleibenden Lagen, insbesondere am Anfang oder am Schluß, soll eine ausgewählt und überprüft werden. Das ergibt den Ansatz (die *'crib'*)

						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24		
						o	b	e	r	k	o	m	m	a	n	d	o	d	e	r	w	e	h	r	m	a	c	h	t		
O	V	R	L	J	B	Z	M	G	E	R	F	E	W	M	L	K	M	T	A	W	X	T	S	W	V	U	I	N	Z	G	Y

mit 24 Vertauschern, die von #1 bis #24 numeriert sind.

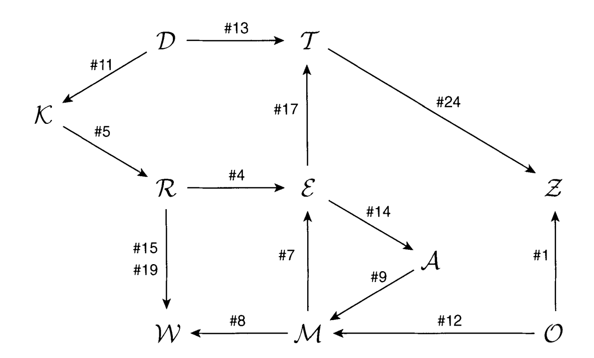


Abb. 156. Ausschnitt aus dem Übergangsgraphen für Beispiel
o b e r k o m m a n d o d e r w e h r m a c h t
Z M G E R F E W M L K M T A W X T S W V U I N Z

Die 24 Übergänge Klartextzeichen–Geheimtextzeichen können in einen gerichteten Graphen komprimiert werden, von dem ein interessierender, vermaschter Ausschnitt in Abb. 156 wiedergegeben ist. Der echt involutorische Charakter der Chiffrierung drückt sich in einer Ergänzung zu einem ungerichteten Graphen aus. Daraus mag ein Teilgraph (im Jargon ein *Menü*) benützt werden für eine rückgekoppelte Verschaltung einer Turing-BOMBE, wie sie Abb. 157 zeigt. Jeder Zyklus in dieser Schaltung bedeutet eine Rückkopplung; ein *Menü* mit 6 Buchstaben und 4 Zyklen ist natürlich „schmackhafter" als eines mit 12 Buchstaben und einem Zyklus, denn es ließ weniger Fehltreffer zu. Entsprechend den 10 ausgewählten Übergängen werden 10 Vertauscher mit 26-adrigen Leitungsschnüren verbunden, und das Testregister wird angeschaltet, sagen wir an dem zentralen Knoten $\mathcal{E}$. An einer gewissen Ader, etwa e, wird Spannung angelegt.

[26] Rotorlage IV I II, Umkehrwalze B. Ringstellung 000,
Steckerverbindungen VO WN CR TY PJ QI. Spruchschlüssel tgv.

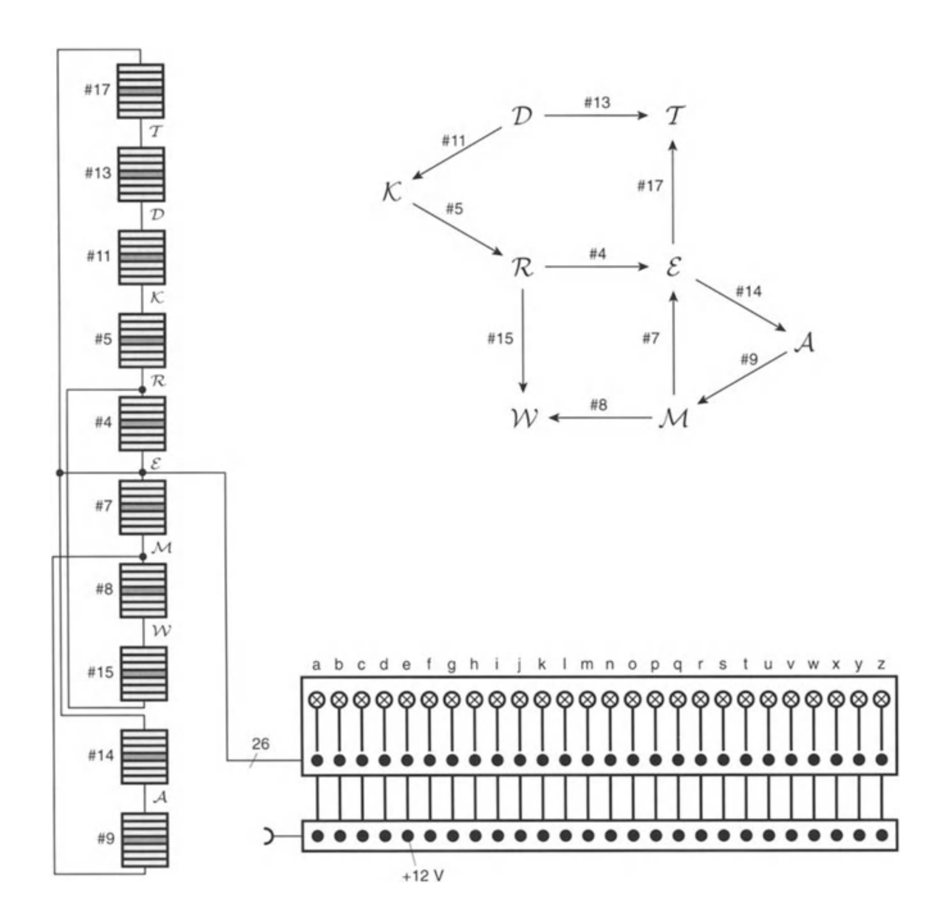


Abb. 157. Turing-BOMBE für Beispiel /oberkommandoderwehrmacht/ (26-adrige Verbindungen)

Die Stellungen 14, 9, 7 bilden eine ‚Schleife' ('*closure*'); es gilt (die inneren Kontakte seien mit $a, b, c, \ldots y, z$ bezeichnet, T bezeichne die Steckerverbindung, P_i die durch den Vertauscher $\#i$ bewirkte Substitution)

$eT = mTP_7$, $mT = aTP_9$, $aT = eTP_{14}$, und damit $eT = eTP_{14}P_9P_7$.

eT ist also ein Fixpunkt von $P_{14}P_9P_7$.

Aber auch die Stellungen 4, 15, 8, 7 bilden eine Schleife; es ist zwar zunächst

$eT = rTP_4$, $wT = rTP_{15}$, $wT = mTP_8$, $eT = mTP_7$;

da aber die Substitutionen *involutorisch* sind, ist auch

$eT = mTP_7$, $mT = wTP_8$, $wT = rTP_{15}$, $rT = eTP_4$, somit
$eT = eTP_4P_{15}P_8P_7$. eT ist also auch ein Fixpunkt von $P_4P_{15}P_8P_7$.

Ferner bilden auch die Stellungen 4, 5, 11, 13, 17 eine ‚Schleife'; es gilt nach geeigneten Involutionen

$eT = rTP_4$, $rT = kTP_5$, $kT = dTP_{11}$, $dT = tTP_{13}$, $tT = eTP_{17}$.

Damit hat auch $P_{17}P_{13}P_{11}P_5P_4$ den Fixpunkt eT .

Angenommen, die Rotorstellung sei nicht die ‚richtige'. Dann breitet sich, durch die Rückkopplung, die Spannung meistens – wenn nämlich genügend viele Schleifen vorliegen – lawinenartig in einer Vielzahl von Durchläufen aus; es werden dadurch nacheinander alle Ausgänge ebenfalls unter Spannung gesetzt, die dort angebrachten Lämpchen leuchten alle auf. Das ist der Widerspruchsfall, der anzeigt, daß die Stellung falsch ist.

Nun sei angenommen, die Rotorstellung ist die ‚richtige', die selbe, mit der chiffriert wurde (wobei also im Beispiel der Vertauscher #4 rT=/r/ in eT=E überführt). Dann gibt es zwei Unterfälle: Wenn die Steckerbrettsubstitution richtig getroffen ist – der unter Spannung gesetzte Eingang e tatsächlich /e/ ist – breitet sich die Spannung nur in einem Durchlauf aus und läßt außer der zu e gehörigen keine Lampe des Testregisters aufleuchten. Eine Relais-Vergleichsschaltung bringt die Maschine zum Anhalten; die Bediener können die Stellung notieren und die weitere Entzifferung versuchen. Ist das aber nicht der Fall, so breitet sich, durch die Rückkopplung, in der *verbleibenden* Schaltung die Spannung wieder meistens – wenn nämlich genügend viele Schleifen vorliegen – lawinenartig aus; es leuchten dadurch alle Lämpchen auf, bis auf eines, das die richtige Steckerbrettsubstitution anzeigt. Auch dann läßt man die Maschine anhalten. Hat man Glück, ist im Haltefall eine passende Rotorenlage gefunden – es kann allerdings auch ein Fehltreffer sein. Das entscheidet sich schnell, wenn man versuchsweise die weitere Umgebung des Chiffrats mit dieser Einstellung entziffert.

Die Möglichkeit dieses Turingschen **Rückkopplungsangriffs** (‘*cycle method*’) wurde von *Gisbert Hasenjäger*, dem für die Sicherheit der ENIGMA zuständigen 23-jährigen Mann im Referat IVa, Sicherheitskontrolle eigener Schlüsselverfahren (*Karl Stein*) der Chiffrierabteilung *Chi* des OKW, nicht gesehen. Dieser Angriff ist, wie oben gezeigt, stark durch den echt involutorischen Charakter der ENIGMA-Chiffrierung begünstigt, würde aber auch für nicht-involutorische Vertauscher funktionieren; beispielsweise für die Schleife

7	9	14
m	a	e
E	M	A

aber solche Schleifen treten erheblich seltener auf. Es müßten also erheblich längere wahrscheinliche Wörter herangezogen werden, oder mehr Stellungen, wie $\mathcal{Z}$ und $\mathcal{O}$ in Abb. 156. Dort könnte beispielsweise das Menü auch durch $\mathcal{U}$, verbunden mit $\mathcal{A}$, oder durch $\mathcal{V}$, verbunden mit $\mathcal{M}$, ergänzt werden. Das würde aber die Anzahl der erforderlichen Vertauscher erhöhen.

19.7.2 *Gordon Welchman* verbesserte *Turing*s Rückkoppelpläne ganz entscheidend, indem er alle Beziehungen, die durch den involutorischen Charakter des für die ENIGMA typischen Steckerbretts (3.2.2) zustandekommen, explizit berücksichtigte.

Wenn *Turing*s BOMBE anhielt, so waren den einzelnen Koppelpunkten wie $\mathcal{A}$, $\mathcal{D}$, $\mathcal{E}$, $\mathcal{K}$ usw. gewisse innere Kontakte zugeordnet. Abb. 158 zeigt eine solche Halte-Konfiguration, die zwei „ungesteckerte“ Zuordnungen $\mathcal{A}$-a, $\mathcal{E}$-e

aufweist. Die beiden Zuordnungen $\mathcal{D}$-t, $\mathcal{T}$-d weisen auf eine Steckerverbindung t-d hin. Die beiden Zuordnungen $\mathcal{W}$-m und $\mathcal{M}$-x widersprechen jedoch der involutorischen Eigenschaft der Steckerverbindung. Die BOMBE hätte in einer solchen Konfiguration gar nicht anhalten sollen, die Sichtbarmachung des hier auftretenden Widerspruchs müßte in die BOMBE eingebaut werden.

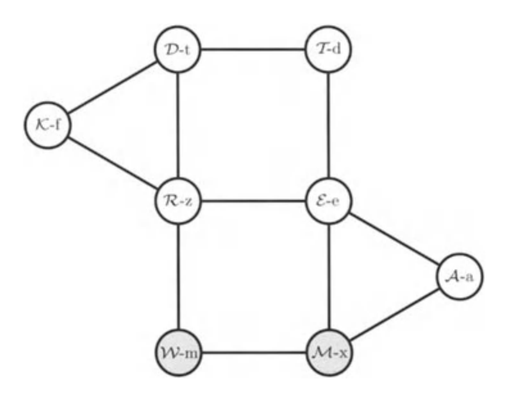


Abb. 158. Unzulässige Halte-Konfiguration

Welchman fand im November 1939 eine einfache schaltungsmäßige Realisierung einer solchen Hüllenbildung hinsichtlich der Involution, das in Abb. 159a auftretende '*diagonal board*'. Zu seiner Wirkungsweise sei auf Abb. 159b verwiesen: Es gilt beispielsweise $eT = dT\,P_{11}P_5P_4$. Der Ausschnitt aus der Schaltung zeigt, wie etwa neben die durch die Vertauscher zustande kommende galvanische Verbindung von e im Bus $\mathcal{E}$ mit d im Bus $\mathcal{D}$ durch das *diagonal board* eine feste galvanische Verbindung von d im Bus $\mathcal{E}$ mit e im Bus $\mathcal{D}$ tritt.

Erst *Welchmans* Verbesserung brachte den Rückkopplungsangriff von *Turing* zur vollen Wirksamkeit und erhöhte die Effizienz der Suche drastisch. Bedeutend weniger Schleifen waren bereits in der Lage, das Testregister aufzufüllen. Das sparte nicht nur Vertauscher, sondern erlaubte auch kürzere Menüs und erhöhte dadurch die Chance, daß der mittlere der drei Rotoren unbewegt blieb. *Welchman* ist so der eigentliche Held der ENIGMA-Geschichte in BP.

Devours und *Kruh* (1985) formulierten es so, daß es *Hasenjäger* trösten mag:

> *"It is doubtful that anyone else would have thought of Welchman's idea because most persons, including Turing, were initially incredulous when Welchman explained his concept"*.

19.7.3 Die Zusammenschaltung der Vertauscher mitsamt dem Testregister und dem *diagonal board* nannten die Leute in *Bletchley Park* wie die Polen 'Bombe', ohne sich tiefere Gedanken über Herkunft des Namens machen zu können. Die erste reguläre Turing-Welchman-Bombe (nach dem Prototyp 'Victory', der noch kein *diagonal board* aufwies) nannte man 'Agnes'[27], sie

[27] *Turing* hatte sie ursprünglich 'Agnus' getauft.

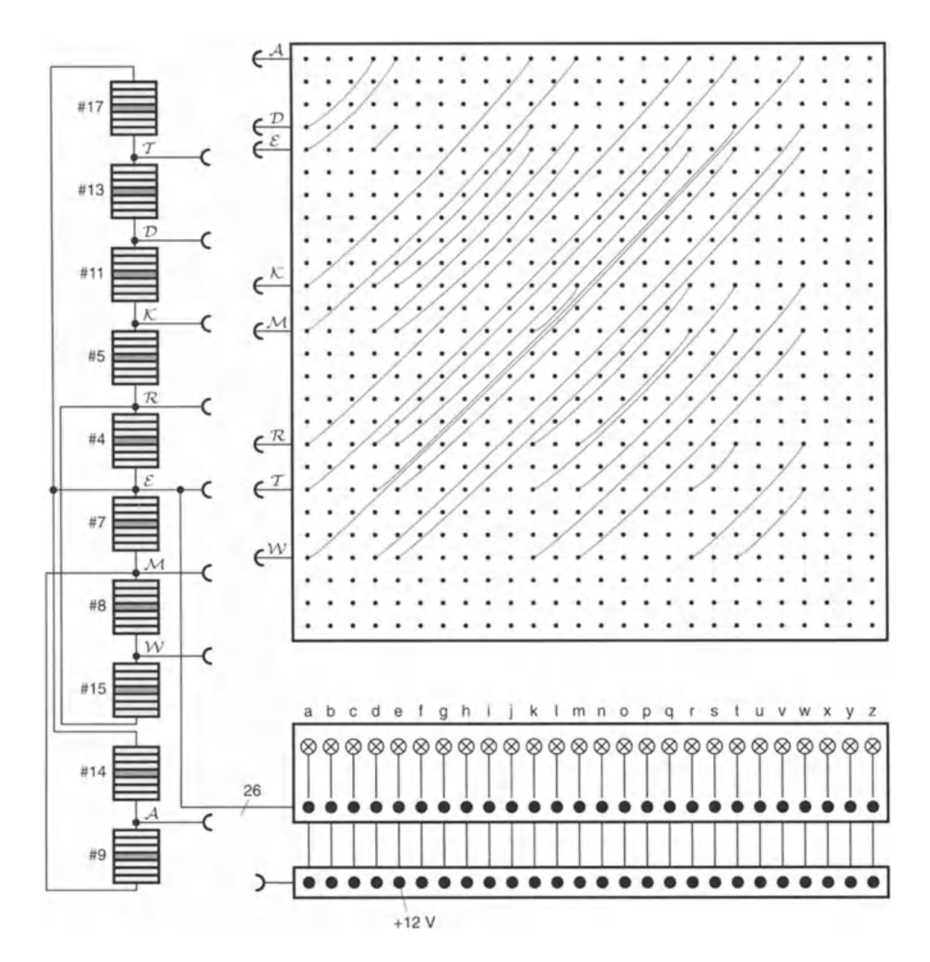


Abb. 159a. Turing-Welchman-BOMBE für Beispiel /oberkommandoderwehrmacht/ (26-adrige Verbindungen)

war Mitte August 1940 betriebsbereit und brauchte etwa 15 Minuten für eine vollständige Durchmusterung *einer* Walzenlage. Im Frühjahr 1941 arbeiteten 8 Bomben ('Ming': Ende Mai 1941), Ende 1941 deren 12. Sie wurden von der British Tabulating Machine Company in Letchworth gefertigt. August 1942 waren 30, März 1943 60 und schließlich 200 Bomben (Abb. 160) im Einsatz.

In den U.S.A. entwickelten sowohl Army wie Navy Hochgeschwindigkeitsbomben, die auch in der Nachkriegszeit noch ihren Dienst taten. Die X-68003 der U.S. Army (SIS), eine von *Sam B. Williams* von *Western Electric* konstruierte reine Relais-Maschine, in Betrieb seit Oktober 1943 und mit 144 Vertauschern ausgestattet, wurde als 'MADAME X' bekannt[28]; sie verwendete Schrittschalter und erlaubte damit eine rasche Veränderung des Menüs. Die Nachbildung der Vertauscher durch Relais war zwar etwas langsam, aber

[28] Es ist unklar, ob der Name eine Anspielung auf *Agnes Meyer Driscoll*, die einsame ENIGMA-Angreiferin von 1940 in OP-20-G, war (vgl. 17.3.4).

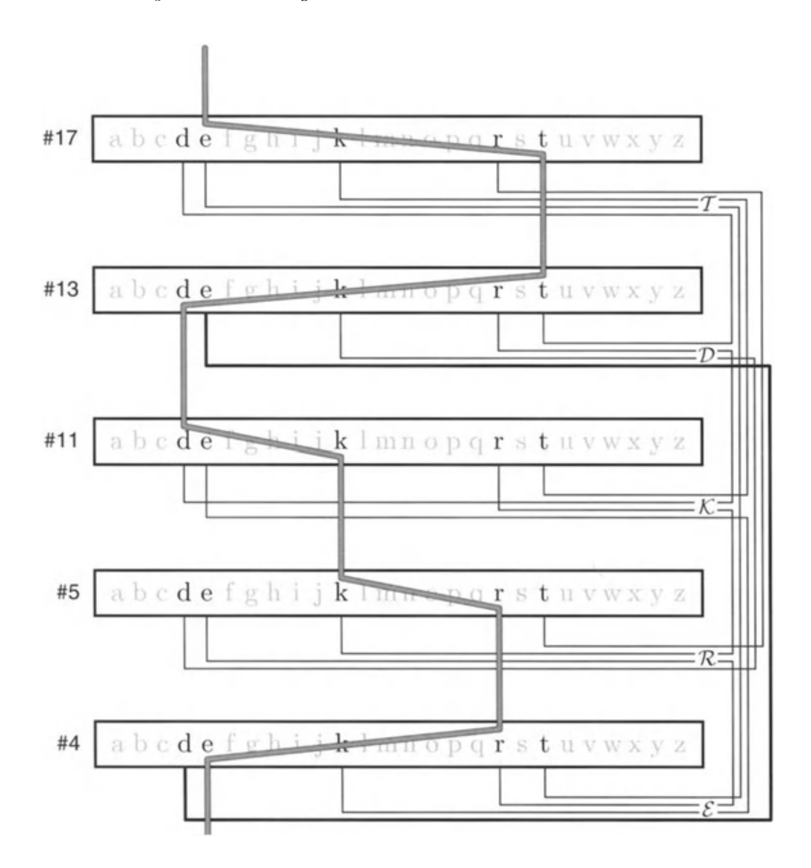


Abb. 159b. Wirkungsweise des *'diagonal board'* von *Welchman* für Beispiel /oberkommandoderwehrmacht/

ohne bewegte Massen. Mit Hilfe der Bell Laboratorien entwickelt, war sie gegen die 3-Rotor-ENIGMAs gerichtet und gegen die 4-Rotor-ENIGMAs der Kriegsmarine schwerfällig. Es wurde nur eine einzige MADAME X gebaut, sie entsprach in der Leistung sechs bis acht britischen Bomben. Entwicklung und Bau verschlangen eine Million $, kostenungünstig im Vergleich zur Navy.

Für OP-20-G der Navy übernahm *Joe Desch* bei NCR, der sich 1940 mit schnellen Schaltungen für Teilchenzähler Kenntnisse in der Elektronik und einen dementsprechenden Ruf erworben hatte, im September 1942 die Aufgabe, ein ehrgeiziges Projekt von 350 Bomben, jede um Größenordnungen schneller als die Turing-Welchman-Bombe, durchzuziehen. Überdies sollten diese Maschinen bis Frühjahr 1943 betriebsfähig sein. *Desch* und seine Gruppe "thought, that American technology and mass production methods could work miracles" (*Burke*).[29] Die Briten konnten nicht mehr tun, als ih-

[29] *Desch* wies jedoch das Ansinnen von *Joseph Wenger*, eine elektronische Version zu bauen, zurück: "An electronic Bombe was an impossibility". Er tat gut daran: Er hätte für eine '*super-Bombe*' mit 20 000 Röhren rechnen müssen, während die Briten für COLOSSUS mit größenordnungsmäßig 2 000 Röhren auskamen.

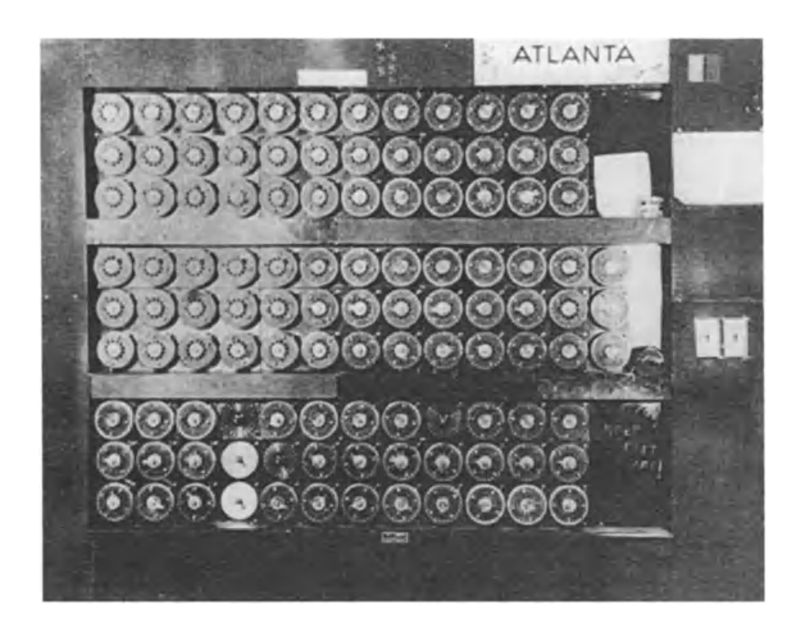


Abb. 160. Britische BOMBE 'Atlanta' (Standardausführung) in Eastcote

rem Alliierten dabei behilflich zu sein. *Howard Engstrom* hatte Juli 1942 *Joe Eachus* nach *Bletchley Park* gesandt. Turing reiste 7. – 13. November 1942 mit der *Queen Elizabeth* über den Atlantik und am 23. März 1943 mit der *Empress of Scotland* zurück. OP-20-G wurde mit Geld und den fähigsten Leuten ausgestattet, dabei war jedoch die Geheimhaltung strenger als die des Atombombenprojekts. NCR in Dayton, Ohio gab den Rahmen. Es ging nicht so schnell wie erwartet, trotz der Bemühungen von *Eachus* waren im Frühjahr 1943 nur zwei Prototypen, ADAM und EVA, halbwegs fertig. *Franklin Delano Roosevelt* gab höchstpersönlich dem Projekt Unterstützung und Beschleunigung. Mittlerweile besserte sich die Lage im U-Boot-Krieg für die Alliierten hauptsächlich aufgrund britischer Entzifferungen. *Desch* hatte insbesondere Probleme mit den schnellaufenden elektromechanischen Vertauschern mit Bürstenabtastung. Mitte Juni 1943 kamen Hoffnungen auf, man würde die Schwierigkeiten bald überwinden. Als am 26. Juli 1943 13 Produktionsmodelle einheitlich nicht funktionierten, sah es dann so aus, als würde das ganze Projekt scheitern. Aber *Desch* gab nicht auf. Die mechanischen Schwierigkeiten wurden Zug um Zug überwunden, die Zuverlässigkeit stieg an. Im September 1943 wurden die ersten von NCR gebauten Maschinen von Dayton nach Washington, dem Einsatzort, verschickt. Mitte November waren 50 Bomben in Betrieb und 30 in Aufstellung. Zum Jahreswechsel war der Erfolg gesichert. Zwar hatte es etwas länger gedauert als optimistischerweise veranschlagt und fast dreimal soviel Geld verschlungen als vorgesehen, aber schließlich kostete eine Desch-Bombe (das Projekt war so geheim, daß sie nicht einmal einen richtigen Namen bekam) nur 45 000 $.

Die 4-Rotor-Bombe der US Navy erhielt 16 Vier-Rotoren-Vertauscher und ein Welchmansches *diagonal board* und war 200 mal schneller als die polnische *bomba*, 20 mal schneller als die Turing-Welchman-Bombe (die Vorgabe war gewesen '26 mal schneller') und immer noch 30% schneller als die gegen die 4-Rotor-ENIGMAs der Kriegsmarine gerichtete halb-elektronische Version 'COBRA' von 1943 der britischen Bombe. OP-20-G hatte aufgeschlossen: Ab Dezember 1943 dauerte die Entzifferung eines ENIGMA-Spruches des ‚Triton'-Netzes im Mittel nur 18 Stunden – es waren 600 Stunden im Juni 1943 gewesen. Gegenüber den britischen Vettern war die Desch-Bombe dadurch ausgezeichnet, daß die Lokalisierung der Vertauscherstellungen und die gesamte Steuerung durch digitale Elektronik mit 1500 Thyratrons (*gas-filled tubes*) geschah. Mindestens 100 Desch-Bomben wurden gebaut. Sie waren so zuverlässig, daß Ende 1943 die gesamte Arbeit am Schlüsselnetz ‚Triton' der U-Boote an die U.S. Navy überging – ein großer Schritt nach den bis 1942 herrschenden Rivalitäten.

Der BRUSA Pakt (*Cooperation in Code/Cipher Matters*) vom Mai 1943 zwischen Großbritanien und den U.S.A., dem das *Travis-Wenger-Agreement* vom Oktober 1942 zwischen GC&CS und OP-20-G voranging, "*began to move the two nations towards a level of unprecedented cooperation*" (Burke) in der Kryptanalyse. Aber einige Reibungen und Spannungen hielten an. "*It was not until the UKUSA agreement of 1946 that the two nations forged that unique relationship of trust that was maintained throughout the Cold War*" (Burke).

Gegen die japanischen (Rotor-)Chiffriermaschinen gerichtete spezielle Maschinen wie VIPER und PHYTON wurden mit Relais und Schrittschaltern aufgebaut; nach und nach bekamen auch sie elektronische Zusätze. Schließlich, gegen Kriegsende, ging man zu ersten elektronischen Maschinen über: OP-20-G baute gegen Japans *kana*-Chiffriermaschine JN-157 den RATTLER, SIS als Nachfolger des AUTOSCRITCHER[30] (ab Anfang 1945) den SUPER-SCRITCHER, OP-20-G wiederum DUENNA, die Briten GIANT – Namen, die bis vor kurzem nicht in der offenen Literatur vorkamen. Die letzteren waren Maschinen, die das Abstreifen der Steckerverbindungen der ENIGMA (14.5.4, 14.5.5) erleichtern sollten. DELILAH schließlich wurde ab September 1943 entworfen, ab Juni 1944 gebaut und war am 6. Mai 1945 gerade fertig.

19.7.4 Die Idee der universellen Rechenanlage, von *Eckert* und *Mauchly* begründet und von *von Neumann* und *Goldstine* zur Reife gebracht, zog jedoch auch die maschinelle Kryptanalysis in ihren Bann. *James T. Pendergrass* empfahl bereits 1946 in einem lange geheimgehaltenen Bericht (zusammen mit *Howard Campaigne*) ihren Einsatz. Es begann im August 1947 mit dem ATLAS-Projekt (vgl. 17.3.5) bei OP-20-G und 1948 mit ABNER

[30] Der Ausdruck 'scritchmus' stammt aus dem Jargon von *Bletchley Park* ("I cannot now recall what technique was nicknamed a 'scritchmus'", schrieb *Derek Taunt*), das Verfahren stammte von *Dennis Babbage*. Für die Ursprünge siehe auch 14.5. Ralph Erskine ist der Meinung, 'scritching' käme von 'scratching out contradictions'.

bei SIS (eine Entwicklung, die 4 Jahre dauerte). Die N.S.A. (*National Security Agency*), die Superbehörde, die Nachfolgerin von SIS und OP-20-G ist, förderte nachdrücklich, wie *Howard H. Campaigne, Samuel S. Snyder und Erwin Tomash* berichteten, die Entwicklung der amerikanischen Rechner-Industrie.

Einige ehemalige Offiziere der U.S. Navy, *Howard T. Engstrom*, *William C. Norris*, und *Ralph Meader* gründeten im Jahr 1946 eine private Gesellschaft, *Engineering Research Associates, Inc.* (E.R.A.), sie wurden durch *Charles B. Tompkins* und *John E. Howard* unterstützt und kooperierten mit *Joseph Eachus* und *James T. Pendergrass* von OP-20-G . Aus Task 13 (ATLAS I), ausgeliefert Dezember 1950, wurde ERA 1101 (Dezember 1951); aus Task 29 (ATLAS II), im letzten Vierteljahr 1953 an die Regierung ausgeliefert, wurde ERA 1103, eine auf dem Markt erfolgreiche Maschine.

E.R.A. ging 1952 in Remington Rand auf. 1954 hielt Remington Rand eine starke zweite Position auf dem Markt mit der verbesserten 1101A (und der UNIVAC II, entwickelt von *Eckert* und *Mauchly*). Der Marktführer IBM kündigte 1951 den *Defense Calculator* an, der als IBM 701 im April 1953 erstmals kommerziell geliefert wurde; IBM's STRETCH entstand aus dem N.S.A. HARVEST von 1962.

1970 gründete *Seymour R. Cray* (1925–1996), ehemals bei E.R.A. unter *Engstrom*, eine eigene Firma und brachte 1976 CRAY-1 mit zahlreichen Nachfolgern heraus (Farbtafel Q). Immer noch bergen die 'sensitiven' Schaltkarten der CRAY-Anlagen die Besonderheiten der kryptanalytischen Ansätze, für die diese Maschinen gebaut sind. Die letzten Reste des Kalten Kriegs haben sich in die Chips verkrochen.

20 Lineare Basisanalyse

"It would not be an exaggeration to state that abstract cryptography is identical with abstract mathematics."

A. Adrian Albert, 1941

20.1 Reduktion linearer polygraphischer Substitutionen

Für lineare polygraphische Substitutionen einer Chiffrierbreite n gelingt in günstigen Fällen eine Reduktion auf eine Exhaustion der Breite n, wenn nämlich eine Zuordnung einer Menge von n häufig auftretenden n-grammen zu einer Menge von n Klartext-n-grammen vermutet werden kann. Insbesondere ist das der Fall, wenn ein längeres wahrscheinliches Wort angenommen wird, das jedoch in n verschiedenen Phasenlagen getroffen wird.

20.1.1 Um die Rechnungen überprüfbar zu halten, beschränken wir uns auf ein Beispiel mit $n = 3$. Es liege folgender Geheimtext vor:

FDYSW IJXNZ NSNRE NHUWA WMQEI EXWSX
ISIGQ JNTAD BWDPU ....

Es sei angenommen, daß den gegebenen Umständen nach eine lineare polygraphische Substitution der Breite 3 über dem Standardalphabet vorliegt – eventuell als zweiter Versuch in einer Reihe von Versuchen mit aufsteigender Breite. Der Geheimtext lautet entsprechend in Trigrammen über $\mathbb{Z}_{26}$

5 3 24 18 22 8 9 23 13 25 13 18 **13 17 4** 13 7 20 **22 0 22** 12 16 4
8 4 23 22 18 23 8 18 8 **6 16 9** 13 19 1 3 1 22 3 15 20 ....

und es sei angenommen, daß die (fett gedruckten) Trigramme **13 17 4** , **22 0 22** und **6 16 9** im weiteren Verlauf des Geheimtextes überaus häufig vorkommen. Angesichts des vorherrschenden Auftretens von /ation/ im Französischen und Englischen kann vermutet werden, daß es sich um die drei Klartext-Trigramme /ati/, /tio/ und /ion/ handelt, bei noch offener Reihenfolge.

In $\mathbb{Z}_{26}$ sind das die Trigramme **0 19 8** , **19 8 14** und **8 14 13** , so daß die Matrix X der linearen Substitution folgendermaßen bestimmt ist, wobei P eine noch unbekannte Permutation ist:

$$\begin{pmatrix} 0 & 19 & 8 \\ 19 & 8 & 14 \\ 8 & 14 & 13 \end{pmatrix} X \quad = \quad P \begin{pmatrix} 13 & 17 & 4 \\ 22 & 0 & 22 \\ 6 & 16 & 9 \end{pmatrix} .$$

Von den sechs Lösungen in $\mathbb{Z}_{26}$ für die $6 = 3!$ Permutationen ergibt nur eine einen vernünftigen Klartext, nämlich

$$\begin{pmatrix} 0 & 19 & 8 \\ 19 & 8 & 14 \\ 8 & 14 & 13 \end{pmatrix} X = \begin{pmatrix} 22 & 0 & 22 \\ 6 & 16 & 9 \\ 13 & 17 & 4 \end{pmatrix} \qquad \text{mit} \qquad X = \begin{pmatrix} 12 & 8 & 17 \\ 8 & 18 & 24 \\ 13 & 19 & 14 \end{pmatrix} .$$

20.1.2 Die Matrix X hat ein alphabetisches Äquivalent, das sich senkrecht gelesen aus dem Kennwort MINISTRYO(F) ergibt. Das bestätigt im Sinn von *Rohrbach* die Entzifferung. Jedoch liegt eine Komplikation vor: Die Chiffrierung X ist nicht injektiv: Der Vektor $(0 \;\; 13 \;\; 0)$ wird von X annulliert. Damit ist bereits die befugte Dechiffrierung nicht eindeutig:

zu 5 3 24 gehören 8 0 5 ≙ i a f und 8 13 5 ≙ i n f ;
zu 18 22 8 gehören 14 4 12 ≙ o e m und 14 17 12 ≙ o r m and so on.

Die polyphone Dechiffrierung lautet:

$$\mathrm{i} \genfrac{}{}{0pt}{}{\mathrm{a}}{\mathrm{n}} \mathrm{f} \quad \mathrm{o} \genfrac{}{}{0pt}{}{\mathrm{e}}{\mathrm{r}} \mathrm{m} \quad \mathrm{d} \genfrac{}{}{0pt}{}{\mathrm{i}}{\mathrm{v}} \mathrm{r} \quad \mathrm{e} \genfrac{}{}{0pt}{}{\mathrm{c}}{\mathrm{p}} \mathrm{t} \quad \mathrm{i} \genfrac{}{}{0pt}{}{\mathrm{b}}{\mathrm{o}} \mathrm{n} \quad \mathrm{o} \genfrac{}{}{0pt}{}{\mathrm{f}}{\mathrm{s}} \mathrm{n} \quad \mathrm{a} \genfrac{}{}{0pt}{}{\mathrm{g}}{\mathrm{t}} \mathrm{i} \quad \mathrm{o} \genfrac{}{}{0pt}{}{\mathrm{a}}{\mathrm{n}} \mathrm{a}$$

$$\mathrm{l} \genfrac{}{}{0pt}{}{\mathrm{e}}{\mathrm{r}} \mathrm{a} \quad \mathrm{d} \genfrac{}{}{0pt}{}{\mathrm{i}}{\mathrm{v}} \mathrm{o} \quad \mathrm{s} \genfrac{}{}{0pt}{}{\mathrm{g}}{\mathrm{t}} \mathrm{a} \quad \mathrm{t} \genfrac{}{}{0pt}{}{\mathrm{i}}{\mathrm{v}} \mathrm{o} \quad \mathrm{n} \genfrac{}{}{0pt}{}{\mathrm{a}}{\mathrm{n}} \mathrm{b} \quad \mathrm{o} \genfrac{}{}{0pt}{}{\mathrm{h}}{\mathrm{u}} \mathrm{t} \quad \mathrm{o} \genfrac{}{}{0pt}{}{\mathrm{h}}{\mathrm{u}} \mathrm{r} \quad \ldots\ldots\ldots \quad .$$

Jeweils die richtige Wahl zu treffen, fällt nicht schwer; die Entzifferung lautet: "inform direction of national radio station about our ... ."

20.2 Rekonstruktion eines durch lineare Iteration erzeugten Schlüssels

Wird ein quasi-nichtperiodischer Schlüssel einer polyalphabetischen linearen polygraphischen Substitution der Breite n durch Iteration einer regulären n-reihigen Matrix A über $\mathbb{Z}_{26}$ generiert (8.6.1), so läßt sich der Rollenwechsel zwischen Nachricht und Schlüssel vornehmen: Ein wahrscheinliches Wort einer Länge k, $k \geq n^2 + n$ wird am Geheimtext entlanggeführt und subtrahiert. Was dabei verbleibt, ist im günstigen Fall ein Stück Schlüssel $(s_{M+1}, s_{M+2}, \ldots s_{M+n^2+n}, s_{M+k})$ einer Länge $k \geq n^2 + n$. Die n Gleichungen

$$\begin{aligned} (s_{M+1}, s_{M+2}, \ldots s_{M+n})\; A &= (s_{M+n+1},\; s_{M+n+2},\; \ldots s_{M+2n}) \\ (s_{M+n+1}, s_{M+n+2}, \ldots s_{M+2n})\; A &= (s_{M+2n+1}, s_{M+2n+2}, \ldots s_{M+3n}) \\ (s_{M+2n+1}, s_{M+2n+2}, \ldots s_{M+3n})\; A &= (s_{M+3n+1}, s_{M+3n+2}, \ldots s_{M+4n}) \\ &\;\vdots \\ (s_{M+n^2-n+1}, s_{M+n^2-n+2}, \ldots s_{M+n^2})\; A &= (s_{M+n^2+1}, s_{M+n^2+2}, \ldots s_{M+n^2+n}) \end{aligned}$$

in $\mathbb{Z}_{26}$ reichen aus, um A zu bestimmen — für $k > n^2 + n$ ergibt sich sogar ein überbestimmtes Gleichungssystem.

Beispielsweise seien die drei Zahlenpaare $(1\ \ 0), (3\ \ 5), (23\ \ 22)$ aus $(1\ \ 0)$ durch zwei Iterationen mit einer Matrix A erhalten; A ist bestimmt durch

$(1\ \ 0)\ A\ = (3\ \ 5)$ und $(3\ \ 5)\ A\ = (23\ \ 22)$ und ergibt sich in $\mathbb{Z}_{26}$ zu

$$A = \begin{pmatrix} 3 & 5 \\ 8 & 17 \end{pmatrix} .$$

Wenn im günstigen Fall die Lage des wahrscheinlichen Wortes paßt, ist das Gleichungssystem sicher auflösbar, für den überbestimmten Fall $k > n^2 + n$ sind mehrere solche Gleichungssysteme auflösbar und geben übereinstimmende Lösungen. Tritt so etwas auf, so liefert es natürlich einen starken Anhaltspunkt. Im ungünstigen Fall, d. h. wenn die Lage des wahrscheinlichen Wortes nicht paßt, ist das Gleichungssystem oder eines der Gleichungssysteme womöglich gar nicht lösbar; ist es jedoch lösbar, so läßt sich der Schlüssel fortsetzen und vom Geheimtext subtrahieren, wobei in aller Regel unvernünftiger Text entsteht und auf diese Weise der Fehlschlag angezeigt wird. Kommt ein genügend langes wahrscheinliches Wort tatsächlich vor, so wird der gesamte Schlüssel bloßgelegt. Fehltreffer sind selten.

20.3 Rekonstruktion eines linearen Schieberegisters

Lineare Schieberegister im weiteren Sinn fallen als Spezialfall unter die Angriffsmöglichkeit von 20.2 . Für sie ist die Iterationsmatrix A (vgl. 8.6.1) eine n-reihige Begleitmatrix,

$$A = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & t_1 \\ 1 & 0 & 0 & \dots & 0 & t_2 \\ 0 & 1 & 0 & \cdots & 0 & t_3 \\ & & \vdots & & & \\ 0 & 0 & 0 & \dots & 0 & t_{n-1} \\ 0 & 0 & 0 & \dots & 1 & t_n \end{pmatrix} .$$

Wird ein Schlüssel durch Iteration mit einer solchen Begleitmatrix erzeugt, so genügt nunmehr bereits ein Stück der Länge $2n$ des Schlüssels, um die Begleitmatrix zu rekonstruieren und damit den ganzen Schlüssel erzeugen zu können.

Um die Rechnungen überprüfbar zu halten, beschränken wir uns auf ein Beispiel mit $n = 4$. Es liege folgender Geheimtext vor:

C G V J F M C I H T X U F S D Y V L M R ... ...

Es sei angenommen, daß den gegebenen Umständen nach die Chiffrierung ein VIGENÈRE ist, wobei der Schlüssel quasiperiodisch ist und durch eine lineare polygraphische Substitution der Breite 4 in $\mathbb{Z}_{26}$ erzeugt wird. Als wahrscheinliches Wort komme den Umständen nach /broadcast/ in Frage.

20.3.1 Die Annahme, das wahrscheinliche Wort liege ganz am Anfang, führt zu dem Ansatz

C	G	V	J	F	M	C	I	H	T	X	U	F	S	D	Y	V	L	M	R	...
2	6	21	9	5	12	2	8	7	19	23	20	5	18	3	24	21	11	12	17	...
b	r	o	a	d	c	a	s	t												
1	17	14	0	3	2	0	18	19												
1	*15*	*7*	*9*	*2*	*10*	*2*	*16*	*14*												

Dies ergibt die Iterationsgleichung in $\mathbb{Z}_{26}$

$$\begin{pmatrix} 1 & 15 & 7 & 9 \\ 15 & 7 & 9 & 2 \\ 7 & 9 & 2 & 10 \\ 9 & 2 & 10 & 2 \\ 2 & 10 & 2 & 16 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & t_1 \\ 1 & 0 & 0 & t_2 \\ 0 & 1 & 0 & t_3 \\ 0 & 0 & 1 & t_4 \end{pmatrix} = \begin{pmatrix} 15 & 7 & 9 & 2 \\ 7 & 9 & 2 & 10 \\ 9 & 2 & 10 & 2 \\ 2 & 10 & 2 & 16 \\ 10 & 2 & 16 & 14 \end{pmatrix}$$

und das überbestimmte Gleichungssystem

$$\begin{pmatrix} 1 & 15 & 7 & 9 \\ 15 & 7 & 9 & 2 \\ 7 & 9 & 2 & 10 \\ 9 & 2 & 10 & 2 \\ 2 & 10 & 2 & 16 \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix} = \begin{pmatrix} 2 \\ 10 \\ 2 \\ 16 \\ 14 \end{pmatrix},$$

das nicht lösbar ist: Die ersten vier Zeilen lassen sich durch Gaußsche Elimination umformen zu

$$\begin{pmatrix} 1 & 15 & 7 & 9 \\ 0 & 1 & 9 & 9 \\ 0 & 0 & 1 & 17 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix} = \begin{pmatrix} 2 \\ 18 \\ 0 \\ 8 \end{pmatrix},$$

mit der durch Rückwärtseinsetzen sich ergebenden Lösung

$$t_4 = 8\,, \quad t_3 = 20\,, \quad t_2 = 0\,, \quad t_1 = 24\,,$$

die aber die fünfte Gleichung offensichtlich nicht erfüllt.

20.3.2 Die nächste zu überprüfende Annahme, das wahrscheinliche Wort beginne mit der zweiten Stelle, führt zu dem Ansatz

C	G	V	J	F	M	C	I	H	T	X	U	F	S	D	Y	V	L	M	R	...
2	6	21	9	5	12	2	8	7	19	23	20	5	18	3	24	21	11	12	17	...
	b	r	o	a	d	c	a	s	t											
	1	17	14	0	3	2	0	18	19											
	5	*4*	*21*	*5*	*9*	*0*	*8*	*15*	*0*											

und zu der Iterationsgleichung in $\mathbb{Z}_{26}$

$$\begin{pmatrix} 5 & 4 & 21 & 5 \\ 4 & 21 & 5 & 9 \\ 21 & 5 & 9 & 0 \\ 5 & 9 & 0 & 8 \\ 9 & 0 & 8 & 15 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & t_1 \\ 1 & 0 & 0 & t_2 \\ 0 & 1 & 0 & t_3 \\ 0 & 0 & 1 & t_4 \end{pmatrix} = \begin{pmatrix} 4 & 21 & 5 & 9 \\ 21 & 5 & 9 & 0 \\ 5 & 9 & 0 & 8 \\ 9 & 0 & 8 & 15 \\ 0 & 8 & 15 & 0 \end{pmatrix};$$

ergibt also das überbestimmte Gleichungssystem

$$\begin{pmatrix} 5 & 4 & 21 & 5 \\ 4 & 21 & 5 & 9 \\ 21 & 5 & 9 & 0 \\ 5 & 9 & 0 & 8 \\ 9 & 0 & 8 & 15 \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix} = \begin{pmatrix} 9 \\ 0 \\ 8 \\ 15 \\ 0 \end{pmatrix},$$

das lösbar ist: Die ersten vier Zeilen lassen sich durch Gaußsche Elimination umformen zu

$$\begin{pmatrix} 1 & 6 & 25 & 1 \\ 0 & 1 & 23 & 7 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix} = \begin{pmatrix} 7 \\ 18 \\ 23 \\ 3 \end{pmatrix},$$

mit der durch Rückwärtseinsetzen sich ergebenden Lösung

$$t_4 = 3, t_3 = 11, t_2 = 4, t_1 = 17,$$

die die fünfte Gleichung offensichtlich erfüllt.

Die Iterationsmatrix zur Fortsetzung des Schlüssels ist somit in $\mathbb{Z}_{26}$

$$A = \begin{pmatrix} 0 & 0 & 0 & 17 \\ 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 11 \\ 0 & 0 & 1 & 3 \end{pmatrix} \quad \text{mit der Inversen} \quad A^{-1} = \begin{pmatrix} 12 & 1 & 0 & 0 \\ 7 & 0 & 1 & 0 \\ 9 & 0 & 0 & 1 \\ 23 & 0 & 0 & 0 \end{pmatrix}.$$

Der Schlüssel kann also ergänzt werden zu

2 5 4 21 5   9 0 8 15 0   15 7 25 4 24   23 20 9 19 3   ...

und führt zu folgender Entzifferung

C	G	V	J	F	M	C	I	H	T	X	U	F	S	D	Y	V	L	M	T	...
2	6	21	9	5	12	2	8	7	19	23	20	5	18	3	24	21	11	12	17	...
2	*5*	*4*	*21*	*5*	*9*	*0*	*8*	*15*	*0*	*15*	*7*	*25*	*4*	*24*	*23*	*20*	*9*	*19*	*3*	...
0	1	17	14	0	3	2	0	18	19	8	13	6	14	5	1	1	2	19	14	...
a	b	r	o	a	d	c	a	s	t	i	n	g	o	f	b	b	c	t	o	... .

("A broadcasting of BBC tonight announced the Allied invasion to be expected within fortyeight hours".)

Die Iterationsmatrix ist aus dem Kennwort (*FID*)*DLER* $\doteq$ (5 8 3) 3 11 4 17 hergeleitet.

Für eine binäre lineare Schieberegister-Chiffrierung in Verbindung mit einem VIGENÈRE über $\mathbb{Z}_2$ gelten entsprechende Überlegungen. Eine Schieberegister-Chiffrierung sollte also nichtlinear sein, um diese Angriffsmöglichkeit zu vermeiden (*Beth* et al. 1982).

21 Anagrammieren

≪Abandonner les méthodes de substitution pour celles de transposition a été changer son cheval borgne pour un aveugle.≫
Étienne Bazeries, 1901

Transpositionen erfreuten sich gelegentlich großer Beliebtheit bei den Militärs, im ausgehenden 19. und angehenden 20. Jahrhundert sowohl bei den preußischen wie bei den französischen Chiffrierdiensten. Sie schienen als 'trench codes' besonders für die unteren militärischen Stäbe geeignet zu sein. *Bazeries* machte sich darüber zu recht lustig und schrieb Transpositionssystemen, die auf den ersten Blick schwierig erschienen, generell eine ≪*complication illusoire*≫ zu. Kryptanalytiker liebten zu allen Zeiten Gegner, die Transposition verwendeten, weil sie ihnen leichte Beute versprachen, gleichzeitig behandelt die Literatur die unbefugte Entzifferung von Transpositionen eher mehr stiefmütterlich.

21.1 Einfache Transposition

Einfache Spaltentransposition (6.2.1), d.h. Umstellung von Einzelzeichen, mit geringer Chiffrierbreite k, kann bei bekanntem k durch gezielte Betrachtung des Kontakts, also von Bigramm-Häufigkeiten, angegangen werden. Für eine halbautomatische Lösung von einfacher Spalten-Transposition und einfacher Block-Transposition gab es im 2. Weltkrieg bei den deutschen Diensten im Auswärtigen Amt (Pers Z) und im OKW besondere Maschinen, genannt ‚Spezialvergleicher' und ‚Bigrammbewertungsgerät' (*Rohrbach, Jensen*).

Dazu wurde ein Textstück (mit einer die Spaltenlänge möglichst nicht übertreffenden Länge) am gesamten Text vorbeigeführt, wobei die auftretenden Bigramme mit eingestellten Bigramm-Häufigkeiten verglichen wurden; in Positionen, in denen die Bigramme besonders gut paßten, hatte man vermutlich aneinanderpassende Textstücke vor sich. Das Verfahren ist im Prinzip auch brauchbar, wenn die permutierten Spalten nicht gleich lang sind.

Für die U.S. Army baute SIS gegen Ende des 2. Weltkriegs FREAK, einen Bigramm-Zähler auf der Basis elektrischer Kondensatoren, ein Ersatz für den 1943 von RCA gebauten MIKE, der von *Burke* als "a huge electromechanical contraption" charakterisiert wurde.

21.1.1 Als Beispiel mag folgender Geheimtext dienen

SSNKL HONIW MMEUN TAHUL INNAH NCINF CIERO
NACBA MZGHN KTHWC DESIN KCAIE ANIM

Häufigkeitszählung ergibt eine gute Annäherung an die Häufigkeiten der deutschen Sprache und legt den Verdacht auf eine Transposition nahe. Die Gesamtzahl von $64 = 8{\times}8$ Zeichen läßt zuerst an eine Spalten-Transposition der Breite 8 mit einer 8×8-Anordnung

S	I	A	H	E	M	W	C
S	W	H	N	R	Z	C	A
N	M	U	C	O	G	D	I
K	M	L	I	N	H	E	E
L	E	I	N	A	N	S	A
H	U	N	F	C	K	I	N
O	N	N	C	B	T	N	I
N	T	A	I	A	H	K	M

denken. Nimmt man deshalb eine Achterspalte, die viele häufige Zeichen enthält, wie etwa die fünfte, ERONACBA, und stellt man sie den anderen Achterspalten gegenüber, so ergeben sich folgende Bigramme (angegeben ist ihre Häufigkeit in %%; wo eine Angabe fehlt, liegt diese unter 0.5%%)

ES 140	EI 193	EA 26	EH 57	EM 55	EW 23	EC 25
RS 54	RW 17	RH 19	RN 31	RZ 14	RC 9	RA 80
ON 64	OM 17	OU 3	OC 15	OG 5	OD 7	OI 1
NK 25	NM 23	NL 10	NI 65	NH 17	NE 122	NE 122
AL 59	AE 64	AI 5	AN 102	AN 102	AS 53	AA 8
CH 242	CU	CN	CF	CK 14	CI 1	CN
BO 8	BN 1	BN 168	BC	BT 4	BN 1	BI 12
AN 102	AT 46	AA 8	AI 5	AH 20	AK 7	AM 28

Die Gegenüberstellung von ERONACBA mit der Spalte SSNKLHON hat deutlich höhere Bigrammhäufigkeiten als die anderen: Bildet man das Produkt aller Häufigkeiten, so ergibt sich der Wert 1.41×10^{14}, während die übrigen Gegenüberstellungen alle Werte unter 3.74×10^{9} ergeben. Wegen der guten Bigramm-Übereinstimmung wird man als nächste die erste Achterspalte SSNKLHON betrachten. Jetzt erhält man mit den restlichen Achterspalten die Gegenüberstellungen

SI 65	SA 36	SH 9	SM 12	SW 10	SC 89
SW 10	SH 9	SN 7	SZ 7	SC 89	SA 36
NM 23	NU 33	NC 5	NG 94	ND 187	NI 65
KM 1	KL 10	KI 7	KH 1	KE 26	KE 26
LE 65	LI 61	LN 4	LN 4	LS 22	LA 45
HU 11	HN 19	HF 2	HK 3	HI 23	HN 19
ON 64	ON 64	OC 15	OT 9	ON 64	OI 1
NT 59	NA 68	NI 65	NH 17	NK 25	NM 23

Diesmal hebt sich die fünfte Gegenüberstellung mit einem Produkt der Häufigkeiten von 3.50×10^{12} nicht mehr so deutlich heraus, aber immerhin noch merklich gegenüber den anderen Gegenüberstellungen, deren Werte alle unter

5.39×10^{11} liegen. Wagt man es, mit der Achterspalte WCDESINK fortzufahren, so ergibt die nächste Gegenüberstellung eine Auszeichnung der Achterspalte AHULINNA. Wenn man die gefundenen Achterspalten sofort auflistet, hat man bis jetzt

ESWA
RSCH
ONDU
NKEL
ALSI
CHIN
BONN
ANKA

und liest flüssig den Klartext. Offensichtlich fügen sich bereits vier der Spalten zusammen, es handelt sich also sogar um eine Transposition der Periode 4. Unterwirft man die verbleibenden Achterspalten der selben Permutation, so erhält man

MICH
ZWAN
GMIC
HMEI
NEAN
KUNF
TNIC
HTMI

und damit den gesamten Text (der als Text „Böll" schon wiederholt auftrat)

eswarschondunkelalsichinbonnankamichzwangmichmeineankunftnichtmi [tderautomatikablaufenzulassendiesichinfuenfjaehrigemunterwegsseinher ausgebildethat] (*Heinrich Böll*, ‚Ansichten eines Clowns', 1963).

21.1.2 Im behandelten Beispiel ergab sich (nicht ganz zufällig) mit der ersten herausgegriffenen Spalte die Anfangsspalte. Das wird im allgemeinen nicht so sein, und man tut gut daran, nach beiden Seiten anschließende Spalten zu suchen. Hat man dabei den Verdacht, auf die End- oder Anfangsspalte gestoßen zu sein, so muß man die Fortsetzung mit einer um einen Platz verschobenen Spalte versuchen. Im übrigen mag es sich, trotz der damit verbundenen Mühe, lohnen, auch Trigrammhäufigkeiten heranzuziehen.

21.1.3 Einfache (periodische) Spaltentransposition bietet nach dem Geschilderten keine Sicherheit, wenn die Periode nicht nahe an die Länge des Textes herankommt; schon einige Wiederholungen erlauben den Angriff nach 21.1.1. Transposition ohne jede Periodizität ist dagegen in aller Regel auch bei beliebig langem Text mehrdeutig lösbar: Ein gewiegter Anwalt könnte also *Brother Tom* von *Jonathan Swift* (6.3) herauspauken, wenn er eine andere Lösung des Anagramms fände. Auch für Transposition ist also ein Einmal-Schlüssel sinnvoll.

21.1.4 Auch ein Code, der einer einfachen Tranposition unterworfen wurde, kann so behandelt werden, wenn man Kenntnisse über die Häufigkeit von Bi-

grammen in den Codegruppen hat. Dies ist beispielsweise der Fall, wenn alle Codewörter, um „aussprechbar" zu sein, aus einem Vokal-Konsonant-System sind, etwa vom Typ $\mathcal{CVCVC}$ (4.4.2) – wie der GREEN Code des U.S. State Department von 1914. Noch im 2. Weltkrieg verwendete das State Department Codes vom $\mathcal{CVCVC}$ und $\mathcal{CVCCV}$ Typ, die Pers Z (*Hans-Kurt Müller*, *Asta Friedrichs*) das Abstreifen einer Überchiffrierung sehr erleichterten.

21.1.5 Weiterhin funktioniert die Methode auch bei gemischter Zeilen-Spalten-Transposition und bei gemischter Zeilen-Block-Transposition (6.2.3) – der Kontakt ist nur gelegentlich zerrissen –, wobei sie zunächst einen zeilenweise permutierten Text ergibt, aus dem sich der Klartext unter Heranziehung des semantischen Inhalts ohne große Mühe ablesen läßt; in unserem Beispiel (bei einer 8 × 8-Anordnung) nach Unterteilung in Achtergruppen

MICHZWAN ALSICHIN ONDUNKEL NEANKUNF
GMICHMEI ESWARSCH TNICHTMI BONNANKA.

Givierge und *Eyraud* haben darauf hingewiesen, daß diese ≪*transposition double*≫ im wesentlichen nicht mehr Schwierigkeiten macht als eine einfache Transposition. Speziell läßt sich die ‚Nihilistenchiffre' (6.2.3) so behandeln, das ≪*double*≫ ist eine *complication illusoire.*

21.2 Doppelte Spaltentransposition

Die doppelte Spaltentransposition (6.2.4) bereitet – außer in Ausnahmefällen – dem unbefugten Entzifferer bedeutend mehr Schwierigkeiten. Das liegt daran, daß nach der ersten Transposition die Kontakte bereits völlig zerrissen sind. *Eyraud* behandelt den Fall recht ausführlich. *Kahn* schreibt:

> *"in theory the cryptanalyst merely has to build up the columns of the second block by twos and threes so that their digraphs and trigraphs would in turn be joinable into good plaintext fragments. But this is far more easily said than done. Even a gifted cryptanalyst can accomplish it only on occasion; and even with help, such as a probable word, it is never easy"*.

21.3 Multiples Anagrammieren

Für den allgemeinsten Fall der Transposition, sogar ohne periodische Wiederholung, gibt es eine allgemeine Methode, die nur die Voraussetzung hat, daß zwei oder mehr Geheimtexte gleicher Länge vorliegen, die nach dem selben Schlüssel chiffriert wurden. Diese Situation einer Klartext-Klartext-Kompromittierung des Schlüssels erlaubt ein Vorgehen parallel zur Methode der *superimposition* von *Kerckhoffs.*

21.3.1 Die Methode beruht darauf, daß gleiche Schlüssel die gleiche Permutation des Klartextes bewirken – das gilt auch für Raster und Würfel. Man schreibt also die Nachrichten untereinander und faßt die dabei auftretenden Kolonnen zusammen. Für die beiden Geheimtextfragmente

GHINT und OWLCN

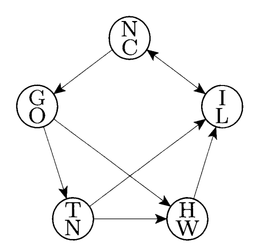
bedeutet das, daß die Paare

G	H	I	N	T
O	W	L	C	N

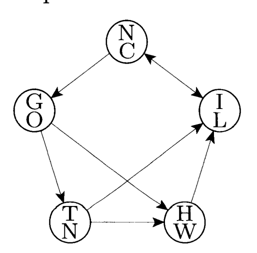
anagrammiert werden. Von den zwanzig Kombinationen zu je zweien zeigen nur die folgenden zwölf Kombinationen (in absteigender Rangfolge)

TH	NG	GT	IN	TI	NI	GH	HI	IG	TN	HT	GI
NW	CO	ON	LC	NL	CL	OW	WL	LO	NC	WN	OL

hinreichend großen Kontakt in beiden Zeilen. Mit vieren dieser Paare, die die besten Kontakte zeigen, läßt sich allerdings nur das semantisch sinnlose $\begin{smallmatrix}\text{INGTH}\\\text{LCONW}\end{smallmatrix}$ bilden und sogar mit den ersten acht Kombinationen erhält man nur zyklische Vertauschungen dieser Lösung, wie aus dem folgenden Graphen mit fünf Knoten und acht Kanten hervorgeht:



Mit der neunten Kombination kommt eine Möglichkeit hinzu, aber die Lösung $\begin{smallmatrix}\text{NIGTH}\\\text{CLONW}\end{smallmatrix}$ ist ebenso sinnlos. Erst wenn man bis zur elften Kombination geht und damit den erweiterten Graphen mit 11 Kanten



erhält, entsteht die sinnvolle Lösung $\begin{smallmatrix}\text{NIGHT}\\\text{CLOWN}\end{smallmatrix}$.

"There will be one order — and only one — in which the two messages will simultaneously make sense" (*Edward S. Holden* 1879).

21.3.2 Multiples Anagrammieren zweier oder mehrerer Geheimtexte kann also als graphentheoretisches Problem betrachtet werden. Eine Mechanisierung ist möglich und angebracht, wenn etwa ein Raster bis hinauf zu 10×10 (6.1.4) ein halbes Dutzend mal verwendet wird. Dieses wird ja in aller Regel vorgefertigt und ist damit zu mehrmaligem Gebrauch bestimmt. Transposition mit festem Schlüssel, und sei sie noch so kompliziert, ist nur der Extremfall von periodischer Transposition, die bereits nicht sicher ist, wenn sie auf Klartext oder auf Text, der noch Häufigkeitsmerkmale zeigt, wie Placode, angewandt wird. Transposition, angewandt auf polyalphabetisch chiffrierten Text (*chiffre à triple clef* von *Kerckhoffs*) widersteht allerdings den besprochenen Methoden — womit nicht gesagt sein soll, daß sie sicher sei. Trans-

position kann auch mit Wörtern anstatt mit Buchstaben geschehen, dann hilft multiples Anagrammieren von Wörtern.

21.3.3 Multiples Anagrammieren wurde erfunden oder doch wenigstens zum ersten Mal der Öffentlichkeit bekanntgemacht 1878 – fünf Jahre vor *Kerckhoffs* – von *John R. G. Hassard* und *William M. Grosvenor*, zwei Herausgebern der New York Tribune, die zusammenarbeiteten, und unabhängig davon von dem schon erwähnten *Holden*, einem Mathematiker des U.S. Naval Observatory in Washington. Der Grund für eine solche massive Anstrengung war ein Skandal im U.S. Senate, dem einige Hundert chiffrierter Telegramme zugrundelagen. Verwendet wurde ein amateurhaftes System von Klartext mit verkleideten Eigennamen und verräterischen Wörtern, der wortweise in ein Raster geschrieben wurde; benützt wurden vier solcher Raster mit 15, 20, 25 und 30 Wörtern. Die Telegramme wurden unabhängig angegangen und übereinstimmend entziffert, was die Authentizität belegte. Die Aufdeckung des Skandals hatte tiefgreifende politische Wirkungen, überdies wurde die amerikanische Öffentlichkeit intensiv mit Geheimschriften und ihrer Entzifferung vertraut gemacht. Vielleicht rührt davon die in den Vereinigten Staaten zu beobachtende Vorliebe für Amateurkryptologie her.

Die Franzosen unter dem damaligen Hauptmann, späteren Oberst und General *François Cartier* hatten jedenfalls ihre Lektion gelernt, als sie sich 1914 dem deutschen Heer gegenübersahen, das als 'trench code' eine doppelte Transposition verwendete. Im Jargon der Franzosen hieß diese Chiffre, die übungshalber schon im Frieden verwendet worden war, *übchi*, weil die Deutschen den Sprüchen stets die Codegruppe ÜBCHI vorangestellt hatten (6.2.4). Den Franzosen gelang es mit multipler Anagrammierung schnell, einzelne Sprüche wenigstens teilweise zu entziffern. Am 1. Oktober 1914 hatten *Cartier* und seine Gehilfen *Adolphe Olivary*, *Henri Schwab* und *Gustave Freyss* erstmals bereits den Schlüssel rekonstruiert. Sie gaben ihn an die französischen Frontstellen weiter, die damit die deutschen Funksprüche so schnell lesen konnten wie die Deutschen selbst. Diese vorteilhafte Situation dauerte bis Mitte November 1914.

Dem Kaiserlichen Heer unterlief dann ein grandioser kryptologischer Fehler: Es wechselte von der widerspenstigen (vgl. 12.4.2) doppelten Transposition zur einfachen Transposition in Verbindung mit einem VIGENÈRE-Verfahren mit dem trivialen dreibuchstabigen Schlüssel $A\,B\,C$, was man im Kopf tun konnte. Diese *complication illusoire* – das Abstreifen der Addition erforderte nur die Betrachtung des Häufigkeitsgebirges, es verblieb also effektiv lediglich eine einfache Transposition – dauerte bis Mai 1915 und kam den Franzosen sehr zustatten.

Obwohl *Le Matin* die Geschichte des französischen Erfolgs vom Oktober 1914 publizierte, kehrte das Kaiserliche Heer Ende 1916 zur Transposition zurück, diesmal unter Benutzung von Drehrastern. Das hielt vier Monate an und brachte natürlich keine Probleme für die französischen Dechiffrierer.

22 Abschließende Bemerkungen

> „Die ungenügende Zusammenarbeit auf dem Gebiet der Entwicklung der eigenen Verfahren, die fehlerhafte Herstellung und Verteilung von Schlüsselunterlagen, unvollständige Schlüsselvorschriften, übersehene Möglichkeiten der Kompromittierung bei der Einführung von Schlüsselverfahren und viele andere Ursachen können dem unbefugten Entzifferer die Möglichkeiten zur Entzifferung fremder Geheimschriften liefern.“
>
> *Erich Hüttenhain*[1], *1978*

Die Geschichte der Kryptologie lehrt, daß der unbefugte Entzifferer von den Fehlern des Gegners lebt (vgl. 11.2.5). Dumme Chiffrierfehler werden von Kryptosekretären (*cipher clerks*) begangen. Taktische und strategische kryptologische Fehler unterlaufen hingegen den Nachrichtenführungsstäben bis hin zu deren Generälen und Direktoren. Dazu gehören auch politische Fragen der Organisation. Die Aufsplitterung der Dienste in Deutschland vor und während des 2. Weltkriegs, nicht zuletzt eine Folge der Rivalitäten zwischen *Ribbentrop*, *Göring* und *Himmler* (Sonderdienst Dahlem in der Abteilung Pers Z des Auswärtigen Amtes, Chiffrierabteilung (*Chi*) im Oberkommando der Wehrmacht, B-Dienst der Kriegsmarine, Forschungsamt des Reichsluftfahrtministeriums, Amt VI E des Reichssicherheitshauptamts) war äußerst nachteilig; die Briten konzentrierten andrerseits von Anfang an ihre Dienste unter dem *Foreign Office* in der *Government Code and Cypher School* und sogar die Militärs fühlten sich nicht schlecht bedient, von den Geheimdiensten M.I.6 (unter *Stewart Menzies*, alias ‘C’) und O.S.S. (unter *David Bruce*) nicht zu reden; die Beteiligten saßen alle in *Churchill*s geheimer “*London Controlling Section*” (L.C.S.) .

Aber bei den Deutschen wie bei den Alliierten *(“need to know”-Doktrin)*[2] bestanden auch aus Gründen nachrichtendienstlicher Sicherheit Abschottungen;

[1] Dr. *Erich Hüttenhain* (26. 1. 1905 – 1. 12. 1990) hatte in Münster Mathematik (bei *Heinrich Behnke*) und Astronomie studiert, er war dann Assistent bei *Lindov*. 1936 wurde er Referent in der Chiffrierabteilung des Oberkommandos der Wehrmacht (OKW); er war zuletzt Leiter der Gruppe IV Analytische Kryptanalyse in der Hauptgruppe Kryptanalyse des seit 1922 dort tätigen Ministerialrats *Wilhelm Fenner*. Nach dem Krieg leitete *Hüttenhain* von 1956 bis 1973 eine Dienststelle der Bundesregierung in Bad Godesberg, die Zentralstelle für das Chiffrierwesen. Sein Nachfolger (1973–1993) war Dr. *Otto Leiberich* .

[2] “A person engaged in classified work was told only enough to enable him to carry out his duties.” (*Brian Johnson* 1978)

sie bewirkten, daß eine Abteilung von den anderen weniger lernen konnte, als es nützlich gewesen wäre, und erlaubten auch manchmal, Mißerfolge und Fehler zu vertuschen.. Zu beurteilen, wie weit solche Umstände den Verlauf von Krieg und Frieden beeinflußt haben, ist mehr Sache der Historiker als der Kryptologen.[3] Eine umfangreiche Publizistik zeigt alle Übergänge von seriösen Berichten bis hin zu enthüllenden Artikeln der Sensationspresse.

22.1 Geglückte Entzifferungen

Die Kryptographie hat ihre eigenen Feinde. Generäle und Botschafter finden manchmal die Mühe nicht wert. Sie können der Ansicht erliegen, daß die Unterordnung unter einen Kryptosekretär Zeitverschwendung und Demütigung ist, und mögen auch begründete Zweifel an der Rechtschaffenheit ihrer Gehilfen haben. Der große Philosoph *François Marie Arouet*, genannt *Voltaire*, ging so weit, daß er die Codebrecher Scharlatane nannte: ≪*ceux qui se vantent de déchiffrer une lettre sans être instruit des affaires qu'on y traite ... sont de plus grands charlatans que ceux qui se vanteraient d'entendre une langue qu'ils n'ont point apprise.*≫ Und der *Earl of Clarendon* schrieb ein Jahrzehnt früher in einem Brief an Doctor *John Barwick* "*I have heard of many of the pretenders of that skill, and have spoken with some of them, but have found them all to be mountebanks.*" 1723 sprach man im *British House of Commons* von einer '*mystery of decyphering*'. Die öffentliche Meinung über Kryptosysteme ist seitdem ein wenig besser geworden. Aber neuerdings muß man stets betonen, daß Kryptanalyse keine Wunder bewirken kann.

Einige Namen erfolgreicher Kryptanalysten sind bekannt geworden, so schon im ersten Weltkrieg die Briten *William R. Hall, Nigel de Grey, Malcolm Hay of Seaton, Oswald Thomas Hitchings*, *G. L. Brooke-Hunt*, die Franzosen *Georges Painvin*, *François Cartier*, *Marcel Givierge*, *E.-A. Soudart*, die U.S.-Amerikaner *Parker Hitt*, *J. Rives Childs*, *Frank Moorman*, *Joseph O. Mauborgne*, *Herbert Osborne Yardley*, *Charles J. Mendelsohn*, der Italiener *Luigi Sacco*, die Österreicher *Maximilian Ronge*, *Andreas Figl*, *Hermann Pokorny* und die Preußen *Ludwig Deubner* und *WilhelmTranow*. Viele andere traten nie ans Licht der Öffentlichkeit und sind vergessen.


Nigel de Grey

Im zweiten Weltkrieg war es sogar eine noch größere Anzahl von Personen, die sich im Codebrechen abmühten; viele nur während der Kriegszeit. In einem kürzlich erschienenen Buch, herausgegeben von *Francis Harry Hinsley* und *Alan Stripp*, finden sich Memoiren von etwa 30 Bletchleyites, wie sie stolz genannt wurden. Es ist weithin zufällig, ob ein Kryptanalyst mit bedeutenden Erfolgen auch bekannt wird. *Fedor Novopaschenny*, der Spezialist für die

---

[3] Für eine seriöse Darstellung siehe etwa *Jürgen Rohwer* und *Eberhard Jäckel* (Hrsg.), ‚Die Funkaufklärung und ihre Rolle im 2. Weltkrieg', Stuttgart 1979.

Sowjetunion bei der deutschen *Chi-Stelle*, *Georg Schröder* beim *Forschungsamt* und *Fritz Neeb* bei der *Heeresgruppe Mitte* liefern Beispiele. *Cort Rave* blieb gänzlich unbeachtet. Auf britischer Seite wurden ab 1974 nach der aufsehenerregenden Publikation von *Frederick W. Winterbotham* eine Reihe von Leuten berühmt, darunter neben *Alan Turing* und *Gordon Welchman* auch *Alfred Dillwyn ('Dilly') Knox*. Auf der Seite der U.S.A ging es nicht so geheimnisvoll zu, neben *Friedman* kamen *Abraham Sinkov*, *Frank Rowlett* und *Solomon Kullback* (Abb. 161) und viele weitere frühzeitig stärker ins Licht der Öffentlichkeit.



Dillwyn Knox (1885–1943)

22.1.1 Über Erfolge der deutschen Seite wurde bisher wenig berichtet. Das hängt sicher auch mit dem Ausgang des 2. Weltkrieges zusammen; man darf daraus nicht schließen, daß es keine gab. Ein Mann, der lange im Hintergrund stand, bevor *David Kahn* seinen Namen in die Öffentlichkeit brachte, ist *Wilhelm Tranow*; vormals Funker in der Kriegsmarine, der schon im 1. Weltkrieg Funksprüche der *Royal Navy* brach und ab 1935 wieder erfolgreich war.



Abb. 161. *William Friedman* (sitzend) mit (von links) *Solomon Kullback*, *Frank Rowlett* und *Abraham Sinkov*

Kahn, ein unvoreingenommener Historiker, schreibt über die Situation Mitte 1943 beim B-Dienst[4] der Kriegsmarine, der unter der Leitung des alterfahrenen und energischen *Tranow* stand: "... *the B-Dienst was at the height of its*

[4] Abkürzung für ,Beobachtungsdienst', hervorgegangen aus dem ,Beobachtungs- und Entzifferungsdienst' der kaiserlichen Marine, deshalb wohl manchmal auch ,χB-Dienst' oder ,xB-Dienst' genannt.

powers, solving 5 to 10 % of its intercepts in time for Dönitz to use them in tactical decisions. Early information sometimes enabled him to move his U-boats so that a convoy would encounter the middle of the pack."

neuen Ausgabe auch einen Verrat-Verdacht zum Anlaß haben. Da aber z.Zt. keins der englischen Hauptverfahren mitgelesen werden kann, besteht keine Möglichkeit genauerer Erkenntnisse auf diesem Gebiet.

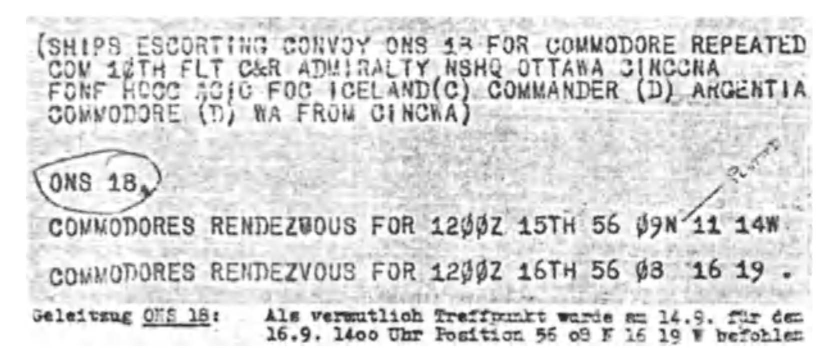
Der erkannte Wechsel des Schlüssels Frankfurt ist durch X-B-Meldung 1145 A an 1.,2. und 3.Skl verbreitet worden.

Im Zusammenhang mit dem Wechsel Frankfurt ist auch der gleichzeitig eingetretene Wechsel der interalliierten Funknamen - siehe KTB 12.6., 1300 Uhr - bemerkenswert.

gez. B o n a t z
Kapt.z.See und Abt.Chef

Abb. 162a . Eintragung im Kriegstagebuch des Chefs der deutschen Marinefunkaufklärung: "Da aber z.Zt. keins der englischen Hauptverfahren mitgelesen werden kann ..." "Der erkannte Wechsel des Schlüssels 'Frankfurt' ist durch X-B-Meldung 1145A an 1., 2. und 3. Skl verbreitet worden..."

In der Tat konnte der B-Dienst von April 1940 an ein Drittel bis die Hälfte der aktuellen *Naval Cipher* mitlesen, einschließlich des ‚Merchant Navy Code'. Als die Briten am 20. August 1940 *Naval Cipher No. 2* (deutscher Deckname „Köln") einführten, wurde dieser Code gegen Ende 1940 teilweise gebrochen und voll von von Februar 1941 an für gut zwei Jahre, also während des Höhepunkts des U-Boot-Krieges,. Damit wurde auch der für die Atlantik-Geleitzugrouten der Alliierten verwendete Code *Naval Cypher No. 3* (deutscher Deckname: „Frankfurt") kompromittiert (Abb. 161a). Zum Abstreifen der Überchiffrierung wurden sechs Hollerith-Tabelliermaschinen verwendet, die halfen, Parallelstellen festzustellen. Gegen Ende 1942 wurden 80% der Funksprüche entziffert, jedoch nur 10% so rechtzeitig, daß sie operationell nutzbar waren. *Dönitz* gab an, daß die Hälfte seiner gesamten Informationen aus dieser Quelle stammte. Sie versiegte erst, nachdem Commander (später Vizeadmiral und Sir) *Norman Denning* in *Bletchley Park* aus entzifferten ENIGMA-Quellen Verdacht schöpfte und die Alliierten am 10. Juni 1943 *Naval Cypher No. 3* aufgaben und anfingen, *Naval Cypher No. 5* zu gebrauchen. Trotzdem gelangen noch weiterhin Entzifferungen (Abb. 162a). Die britische Führung konnte sich, wie die deutsche, nur sehr schwer zu der Überzeugung durchringen, daß ihre Chiffrierung gebrochen war. *Patrick Beesly* gibt *Bletchley Park* die Schuld, wo man offensiv eingestellt war und wenig für die Sicherheit der eigenen Chiffrierverfahren tat. *Colin Burke* berichtet von Rivalitäten und gedrosseltem Informationsfluß zwischen dem Vereinigten Königreich und den Vereinigten Staaten 1942. Für die Kriegsmarinen endete das im Oktober 1942, für die Armee dauerte es bis ungefähr September 1943 (vgl. 19.7.3); schließlich entwickelte sich jedoch eine beispiellose, von gegenseitigem Vertrauen getragene Zusammenarbeit.


(SHIPS ESCORTING CONVOY ONS 18 FOR COMMODORE REPEATED
COM 10TH FLT C&R ADMIRALTY NSHQ OTTAWA CINCCNA
FONF HCOC AOIC FOC ICELAND(C) COMMANDER (D) ARGENTIA
COMMODORE (D) WA FROM CINCWA)

ONS 18

COMMODORES RENDEZVOUS FOR 1200Z 15TH 56 09N 11 14W

COMMODORES RENDEZVOUS FOR 1200Z 16TH 56 08 16 19 .

Geleitzug ONS 18: Als vermutlich Treffpunkt wurde am 14.9. für den 16.9. 14oo Uhr Position 56 o8 N 16 19 W befohlen

Abb. 162b. Vergleich eines Funkbefehls des CINCWA vom 14. September 1943 an Geleitzug ONS 18 mit Entzifferung durch den B-Dienst der Kriegsmarine: ‚Treffpunkt 16.9. 1400 Uhr [deutsche Sommerzeit] Position 56 08 N 16 19 W‘

Es wurde oft die Frage gestellt: Wurde die Schlacht auf dem Atlantik durch Kryptanalyse entschieden? Jürgen Rohwer und Harry Hinsley haben darauf hingewiesen, daß die Situation ziemlich ausgeglichen war, solange die Briten zu einen defensiven Seekrieg gezwungen waren. Erst um die Mitte 1943, als die allierten Seestreitkräfte stark genug waren, den anti-U-Boot-Krieg offensiven zu führen, gerieten die deutschen U-Boote zusehends in Bedrängnis.

Die Erfolge des B-Dienstes hatten Tradition: Zu Kriegsbeginn las er bereits die *Naval Cypher No. 1*, einen 4-ziffrigen überchiffrierten Code; das wurde ihm ermöglicht durch eine 1935 im Abessinienkrieg erfolgte Kompromittierung mit dem 5-ziffrigen, weithin benutzten Naval Code, der bereits gebrochen war. Bei der Eroberung Norwegens im April-Mai 1940 gelang es der Kriegsmarine stets, ein genaues Bild der Situation in der British Admiralty zu haben, bis eine Änderung der Chiffrierung im August 1940 den B-Dienst zeitweilig zurückwarf. *Kahn* zitiert eine anonyme Quelle “*If one man in German intelligence ever held the keys to victory in World War II, it was Wilhelm Tranow.*” Daß es keine Schlüssel zu diesem Sieg gab, dafür hatte *Hitler* gesorgt.

Die Reichswehr brach, *Hüttenhain* zufolge, Anfang der dreißiger Jahre den Verkehr des französischen Kriegsministeriums mit den französischen Wehrkreisen. Die Chiffrierung war allerdings miserabel: Ein über lange Jahre festbleibender numeraler Code wurde periodisch mit einem VIGENÈRE mod. 10 überchiffriert, die Periode schwankte zwischen 7 und 31. Alle Sprüche konnten mitgelesen werden. Lediglich im Verkehr mit dem an Italien angrenzenden Wehrkreis wurde ein anderes Verfahren verwendet, ein anderer Code mit einer Transposition als Überchiffrierung. 1938 gelang Chi auch hier der Bruch. Das französische Kriegsministerium verfügte, daß dieses Verfahren auf alle Wehrkreise ausgedehnt wurde, als am 3. September 1939 der Krieg mit Deutschland ausbrach. Damit konnten die Deutschen sofort den ganzen französischen Dienstverkehr mitlesen, was ihnen im Frankreichfeldzug im Juni 1940 große Vorteile brachte. Frankreich hatte den Fehler (11.1.3) gemacht,

ein Chiffrierverfahren, das bereits längere Zeit in einem kleinen Bereich benutzt wurde, zum Hauptverfahren für einen großen Bereich zu machen.


Hans Rohrbach (1903–1993)

Der Erfolg, den *Hans Rohrbach* von 1942 bis September 1944 gegen das Streifenverfahren der U.S.-Diplomatie erzielte, wurde schon in 14.3.6 geschildert. In 14.6 wurde auf die Rolle, die die sogenannten CQ-Funksprüche des State Departments in Washington spielten, hingewiesen.

Demgegenüber bescheiden war der in 19.4.1 erwähnte Erfolg gegen den rumänischen Militärattaché. Militärattachés scheinen besonders beliebte Angriffsziele zu sein: Als *Rommel* in Nordafrika gegen die britische 8. Armee *Montgomerys* kämpfte, konnte in Berlin im Herbst 1941 die Chiffrierung des amerikanischen Militärattachés in Cairo, Oberst *Frank Bonner Fellers* (später Brigadegeneral und Führungsgehilfe von General *Douglas Mc Arthur*) entziffert werden – teils weil *Fellers* die unausrottbare Gewohnheit hatte, sein Sprüche stereotyp beginnen zu lassen, teils weil Italien, damals noch im Frieden mit den U.S.A., in der amerikanischen Botschaft in Rom das Codebuch zum Kopieren „auslieh“. *Fellers* meldete im brandneuen Code BLACK täglich unter anderem die Pläne der 8. Armee für den nächsten Tag, *Rommel* konnte stets innerhalb weniger Stunden bedient werden. Die U.S.A waren kryptologisch ein unsicherer Verbündeter Großbritanniens. Italien versuchte vorsichtiger zu sein: Der Chef des Nachrichtendienstes, General *Cesare Amè*, überließ den Deutschen nicht das Codebuch, sondern nur die Entzifferungen. Mit dieser Klartext-Geheimtext-Kompromittierung gelang aber Berlin die Rekonstruktion des Codebuches. Der Bruch hatte im Juni katastrophale Folgen für einen für Malta bestimmten Geleitzug; *Bletchley Park* schöpfte wieder einmal Verdacht und *Fellers* mußte seinen Posten verlassen. Trotzdem wurde er mit der *Distinguished Service Medal* ausgezeichnet. Er war fast so schlimm wie *Murphy*.

Die Funker der U.S.Army waren im Gebrauch ihrer Hagelin-Maschinen, der M-209, ebenso undiszipliniert wie ihre deutschen Kollegen: als Spruchschlüssel von 6 Buchstaben wählten sie vorzugsweise Vornamen ihrer Liebchen, und so meistens einen Tag lang immer wieder den selben Schlüssel. Solche phasengleichen Chiffrierungen ermöglichten *Erich Hüttenhain* fortwährend den Einbruch in die ohnehin nicht sehr sichere, involutorische Beaufort-Chiffrierung. Generalfeldmarschall *Erwin Rommel* „hat davon profitiert“ (*Otto Leiberich*).


Erich Hüttenhain (1905–1990)

22.1.2 Japan versuchte, neben chinesischen hauptsächlich amerikanische Codes zu brechen. Allzu schwer war das nicht, da trotz *Yardleys* Warnung (8.5.6) die U.S. Diplomatie leichtsinnig blieb: Unter *Roosevelt* wurde ein neuer Code, BROWN eingeführt. Er fiel bald darauf einer Bande von Ein-

brechern in Zagreb in die Hände, war also nachweislich kompromittiert. Da es sich offenbar ‚lediglich' um Kriminelle handelte, wurde BROWN nicht aus dem Verkehr gezogen. Und *Stanley K. Hornbeck* schrieb seinem Chef, dem Secretary of State *Stimson*: "*Mr. Secretary: I have the feeling that it is altogether probable that the Japanese are 'breaking' every confidential telegram that goes to and from us*". Die Unsicherheit amerikanischer diplomatischer Codes wurde als unvermeidlich hingenommen. Da nimmt es nicht wunder, daß der Entzifferungsdienst des japanischen Außenministeriums, *angō kenkyū han*, gelegentlich einfachere Codes – GRAY beispielsweise – entziffern konnte. Mit BROWN gelang es ihm und auch *toku mu han*, dem Entzifferungsdienst des Admiralstabs, nicht. Da mußte schon ein Einbruch helfen: Unter der Führung von Hauptmann *Hideya Morikawa* wurde gegen Ende 1937 im amerikanischen Konsulat in Kobe der BROWN Code und das Schiebergerät M-138 photographiert, dessen Aussehen den Japanern bis dahin unbekannt war. Es gelang ihnen aber nicht, den M-138-Verkehr mitzulesen. *toku mu han* stürzte sich dann auf das verwandte Schiebergerät CSP-642 der U.S. Navy (14.3.5). Ihre Ausbeute war gering, weil sie methodisch rückständig waren. Von den Deutschen hatten sie jedoch den BAMS Code (4.4.5) erhalten, den diese am 10. Juli 1940 durch ihren Hilfskreuzer *Atlantis* auf dem britischen Dampfer *Automedon* erbeutet hatten. Die Japaner brauchten also nur die Überchiffrierung abzustreifen, was ihnen natürlich gelang.

In der umgekehrten Richtung war mehr Erfolg zu verzeichnen. Die U.S.A., die die Hauptlast des Kriegs der Alliierten im Pazifik trugen, hatten auch die meisten Erfolge in der Entzifferung japanischer Funksprüche zu verzeichnen. Daß die japanische Sprache für den westlichen Kulturkreis zunächst fremdartig und undurchdringlich erscheint, schützte jedenfalls Japan nicht vor der Entzifferung seiner Geheimnisse. Die Amerikaner durchlöcherten japanische Codes und Chiffrierungen in den zwanziger (*Yardley*), dreißiger (*Holtwick*) und vierziger Jahren (*Rosen*). Es gibt zuverlässige Berichte (19.3.2), wonach auch die deutsche Seite die japanische PURPLE-Chiffrierung ständig brach.

Abgesehen von den spektakulären '*Venona breaks*' (8.8.7) weiß man wenig über Erfolge der U.S.A. im Brechen sowjetrussischer Chiffrierungen während des Kalten Kriegs. Im Jahre 1972, während der Gespräche zur Begrenzung strategischer Waffen, gelang den Amerikanern ein Treffer, aber das war ein glücklicher Zufall ("... but the solution was a fluke, made possible by a Soviet enciphering error", *Kahn*). So etwas gelingt hie und dann. Und wenn es öfter gelungen sein sollte, gab es Grund genug, sich nicht damit zu brüsten.

22.1.3 Die Sowjetunion hatte, obschon der Schwerpunkt ihrer nachrichtendienstlichen Bemühungen auf Abhören, Ausspähen, Diebstahl und Erpressung beruhte, auch im Kalten Krieg kryptanalytische Erfolge, so etwa gegen die Schweizer Diplomatie, die mit Hagelin-Maschinen arbeitete, und ähnlich gegen Italien — von kleineren Nationen ganz abgesehen.

Gegen Ende des 2. Weltkriegs nahm auch die Zahl der von der Roten Armee erbeuteten ENIGMA-Schlüsselunterlagen derart zu, daß der Prozent-

satz ihrer Erfolge gegen den ENIGMA-Verkehr der deutschen Wehrmacht beträchtlich wurde. Jedoch gab es allem Anschein nach keine den polnischen, britischen und U.S.-amerikanischen Bomben vergleichbare Codebrechermaschinen. Zur Zeit des Kalten Krieges war die Sowjetunion, *Louis Tordella* zufolge, sogar gegen die von der NATO verwendete KW-7 erfolgreich. *David Kahn* spürte 1992 einen zwischenzeitlich in England lebenden Russen, *Victor Makarov*, auf, der als Übersetzer Einblicke in die Tätigkeit des 16. Direktorats des KGB (Direktor: General *Andrei Nicolayevich Andreyev*) gewonnen hatte. Von ihm und durch späteren Kontakt mit *Andreyev* erfuhr *Kahn* etliche Details, so etwa daß die sowjetische Kryptanalyse unter *Sergei Tolstoy* ab Ende 1941 gegen die japanische PURPLE erfolgreich war, und auch, daß das KGB einen Supercomputer, SWORD genannt, für Kryptanalyse benutzte. Ein technisch komplettes Bild der sowjetischen Kryptanalyse fehlt jedoch.

22.2 Arbeitsweise des unbefugten Entzifferers

„Es ist natürlich nur die Arbeit des *unberufenen* Entzifferers, die mathematisch von Interesse ist, wobei überdies an einen erfahrenen Entzifferer gedacht ist. Die Erfahrung im Entziffern muß durch langjährige Übung erworben werden. Hierbei wird sich der Entzifferer je nach Anlage und Neigung zu einem mehr sprachlich oder zu einem mehr mathematisch geschulten entwickeln. Lösungen von genügend komplizierten Verfahren sind Gemeinschaftsarbeit mehrerer Entzifferer beider Richtungen, deren jede wieder besondere Spezialisten hat. Die Mathematiker benötigen insbesondere Spezialisten für maschinelle Methoden.“

Hans Rohrbach 1949

“*Deciphering is an affair of time, ingenuity, and patience*”

Charles Babbage 1864

“*The cryptographer's main requisites are probably patience, accuracy, stamina, a reasonable clear hand, some experience, and an ability to work with others.*”

Christopher Morris 1992

Da ich kein professioneller Entzifferer bin, fällt es mir sowohl schwer wie leicht, mich abschließend über die Arbeitsweise des unbefugten Entzifferers zu äußern. Schwer, weil ich meine eigenen Erfahrungen nicht mit Schweiß und Tränen gesammelt habe. Leicht, weil ich dabei nicht in Gefahr bin, durch Erfolge geblendet oder durch Mißerfolge verbittert zu sein. Jedenfalls kann man der Literatur entnehmen, daß berufsmäßige Entzifferer kein leichtes Leben haben. *Rejewski*, beispielsweise, ging nach Polen zurück und zog einer Universitätslaufbahn die Stellung eines kaufmännischen Direktors vor. *Alastair Denniston* gab seinem Sohn *Robin* den Rat: “*Do what you like to do, but don't do what I do.*” *Robin Denniston* wurde Verleger. Manchem mag es schwer gefallen sein, zwanzig, dreißig und vierzig Jahre lang absolutes Stillschweigen bewahren zu müssen; sogar in Situationen wie der von *Jack Good*, der in einem Hotel in der Nähe von *Bletchley Park* einquartiert

wurde und dem ein pensionierter Bankbeamter eine lebhafte Beschreibung einer kommerziellen ENIGMA gab, die seine Bank in seiner früheren Zeit benutzt hatte.

22.2.1 Die Arbeit eines professionellen Entzifferers ist undankbar, es ist ihm nicht erlaubt seine Erfolge öffentlich oder auch nur im Kreise seiner Fanilie zu feiern; ja nicht einmal seine engsten Angehörigen dürfen wissen, was er tut. Er steht ständig in der Gefahr, entführt oder erpreßt zu werden. Die damit verbundenen Beschränkungen bestehen üblicherweise auch nach Beendigung seines aktiven Dienstes.

Andrerseits hat *Ralph V. Anderson*, der im Jahre 1940 den *code room* des U.S. Navy Department in Washington, D.C. betrat und 1946 in kryptologischen Funktionen an das Department of State überwechselte, wo er für mehr als zwanzig Jahre diente, bekannt: "*If I had been given the choice of any position I wanted, I would have chosen the one I had.*" Jedem das seine.

22.2.2 Schwierig finde ich es, allgemeine Aussagen über anzuwendende Methoden zu machen. Der Rat von *Bazeries*, der ein sehr erfolgreicher Kryptanalyst war, ≪*changer son fusil d'épaule*≫, ist allerdings nur für Leute bestimmt, die genügend Phantasie haben. Man darf keine Scheuklappen haben, keine eingefahrenen Geleise benutzen. Das Beispiel von *Turing* und *Welchman* zeigt es: In ihrer Unerfahrenheit lag ihre Stärke. Damit waren sie besser als *Dillwyn Knox*, der viel erfahrener war, aber auch weniger wagemutig. Als Mannschaft waren *Turing* und *Knox* unschlagbar, und sogar *Turing* und *Welchman* erzielten mehr als die Summe ihrer einzelnen Leistungen.

Eines wird jedenfalls dem erfolgreichen unbefugten Entzifferer nicht passieren: Er wird sich nicht abschrecken lassen von der angeblichen Komplexität der Aufgabe. Die Polen waren erfolgreich, weil sie eine von Hand zu zeitraubende Analyse automatisierten und damit die Erwartungen von Chi, wie lange es dauern würde, durch Parallelisierung um den Faktor sechs und durch Mechanisierung mindestens um den Faktor zwanzig unterboten. Die Welchman-Bombe gar macht, wie *Welchman* nicht ohne Stolz sagte, Trillionen von Möglichkeiten der Steckerverbindungen belanglos, weil sich die lawinenartige Ausbreitung der Spannung in einer vergleichsweise einfachen Schaltung "*in less than a thousandth of a second*" bewerkstelligen läßt.

22.2.3 Im Prinzip gibt es unendlich viele kryptanalytische Methoden. Nachfolgend nun eine zusammenfassende Übersicht über die Strategie des Angriffs.

22.2.3.1 Die reinste Form der unbefugten Entzifferung (*'pure cryptanalysis'*) macht keinerlei Voraussetzungen; sie braucht auch den Linguisten nicht, denn sie ist mathematisch von Natur. Wie *David Kahn* sagte, funktioniert sie im Prinzip sogar für eine dem Entzifferer nicht bekannte Sprache, etwa der letzten Zwischensprache bei einer Komposition von zwei oder mehr Verfahren, wie überchiffrierter Code bei unbekanntem Codebuch. Reine Kryptanalyse ist direkt geeignet für maschinelle Durchführung und kann in der

Form eines Rechnerprogramms beschrieben werden. Reine Kryptanalyse benötigt jedoch, und das ist ihre Schwäche, in der Regel längere Geheimtexte als jede der übrigen Methoden. In einigen Fällen einer Klartext-Klartext-Kompromittierung, beispielsweise der Periodenbestimmung für eine polyalphabetische Chiffrierung (18. Kapitel) oder der phasengerechten Ausrichtung einiger polyalphabetisch, mit verschiedenen Schlüsselanfängen, chiffrierter Texte, wie auch im Fall einer Geheimtext-Geheimtext-Kompromittierung (19. Kapitel), bewirkt reine Kryptanalyse die Reduktion zu einer monoalphabetischen, möglicherweise polygraphischen Zwischensprache, einer Chiffrierung der Klartextsprache, die bedenkenlos den Klauen des Linguisten überlassen werden kann.

22.2.3.2 Reine Kryptanalyse ist ein Spezialfall eines Angriffs (*'ciphertext-only attack'*, *'known ciphertext attack'*), der lediglich Überlegungen und Annahmen über die *Art* der zugrundeliegenden Sprache einbezieht. Beispielsweise wird zunächst nur die *Verteilung* der Einzelzeichen-Häufigkeiten festgestellt. Ist es die einer bekannten natürlichen Sprache, können alle Chiffrierverfahren ausgeschlossen werden, die Häufigkeiten nivellieren, insbesondere echt polygraphische (sofern sie nicht Häufigkeiten vortäuschen, vgl. 4.1.2) und echt polyalphabetische Chiffrierungen; unter den verbleibenden sind funktionale einfache Substitutionen, Transpositionen und deren Kompositionen. Sind sogar die einzelnen Häufigkeiten die einer gewissen natürlichen Sprache, können auch echte einfache Substitutionen ausgeschlossen werden; unter den verbleibenden sind Transpositionen wie auch solche polygraphische Substitutionen, die die Häufigkeiten eben dieser Sprache vortäuschen. Die Häufigkeitsuntersuchung (15. Kapitel) eignet sich somit sowohl zum Brechen einer monoalphabetischen Substitution wie zum Abstreifen einer einfachen Substitution von einer Transposition.

Ist aber die Verteilung der Einzelzeichen-Häufigkeiten nivelliert, so besteht umgekehrt (wenn man den Gebrauch von Homophonen ausschließen kann) *Verdacht* auf eine polyalphabetische Chiffrierung und/oder auf eine polygraphische Chiffrierung. Beiden Möglichkeiten muß nachgegangen werden. Für den ersten Fall ist (vgl. 17. Kapitel) Periodenbestimmung angezeigt – mit der Aussicht auf Reduktion zu einer monoalphabetischen einfachen oder auch echt polygraphischen Substitution. Gelingt dies nicht, so könnte bereits eine monoalphabetische polygraphische Substitution vorliegen; es könnte sich aber auch um eine fortlaufende polyalphabetische Chiffrierung handeln. In diesem, unter den heutigen Umständen realistischen Fall ist Superimposition angezeigt, sofern eine Klartext-Klartext-Kompromittierung vorliegt.

22.2.3.3 Viel stärker linguistischer Natur sind die Methoden, die auf partiellen oder totalen Klartext-Geheimtext-Kompromittierungen beruhen. Die Methoden der Mustererkennung (13., 14. Kapitel) verlangen zumindest Hinweise auf wahrscheinliche Wörter oder Phrasen; im besten Fall erhält man solche aus einer Klartext-Geheimtext-Kompromittierung. Zur Erzielung einer solchen ist Schläue angebracht. Schläue ist erforderlich beim Finden

guter wahrscheinlicher Wörter. Dazu gehört auch Einfühlungsvermögen in die Denk- und Redensarten des Gegners. Bei den Briten in *Bletchley Park* waren Champions bei der Zubereitung der *cribs* (vgl. 19.7) der linguistisch orientierte Mathematiker *Shaun Wylie* und die Philologin *Hilary Hinsley née Brett-Smith*. Es gab aber auch Leute mit einer Art abstrakter Fähigkeit, Muster aufzuspüren, wie der Schachchampion *Hugh Alexander* und die formal begabte Germanistin *Mavis Batey née Lever*[5] , die mit großem Geschick dem *banburismus* (19.6.4.3) huldigten.

Es gehört natürlich dazu, daß der unbefugte Entzifferer über alle Erkenntnisse der Aufklärung verfügt, auch über solche, die durch andere unbefugte Entzifferer erzielt wurden, und vor allem über solche, die durch andere Methoden – Befragung von Gefangenen, Aushorchung der Bevölkerung, Abhören und Spionage erzielt wurden. Diese Forderung läßt sich kaum mit allgemeinen Sicherheitsmaßnahmen verbinden (*“need to know”-Doktrin*) und schon gar nicht unter politischen Maßstäben realisieren – im 2. Weltkrieg hätte dann *Churchill* am besten selbst die *cribs* zubereitet.

Diesem Normalfall des ‘*known plaintext attack*’ steht gegenüber die Herbeiführung einer Klartext-Geheimtext-Kompromittierung durch List (‘*chosen plaintext attack*’). List ist unerschöpflich: Vorfälle, über die berichtet wurde, variieren von solchen, bei denen ein bestimmter Vorfall ausgelöst wurde („erloschen ist leuchttonne“, vgl. 11.1.3, Fußnote 2), bis zu solchen, bei denen dem Gegner eine Nachricht unterschoben wurde (das japanische Kuckucksei, 11.1.2; *Figl*s Zeitungsfutter, 11.1.2).

Sogar eine Geheimtext-Geheimtext-Kompromittierung ist in dieser Weise nützlich, wenn das eine System schon gebrochen ist, weil dann eine Zurückführung auf eine Klartext-Geheimtext-Kompromittierung gelingt. Zu einer solchen Fortsetzung eines Bruches wurden beispielsweise in Bletchley Park Notsituationen des Gegners herbeigeführt (‚Gartenpflege‘, 19.4.1).

22.2.3.4 Eine besondere Angriffsart (‘*chosen ciphertext attack*’) besteht bei asymmetrischen Chiffrierverfahren, die den Schlüssel zur Chiffrierung offenlegen (‚öffentliche Schlüssel‘), wenn das Funktionieren eines eingriffsresistenten ‘schwarzen Kastens’ zur Dechiffrierung aufgedeckt werden soll, also der private Schlüssel gesucht wird.

22.2.4 Geheimtext-Geheimtext-Kompromittierung ist besonders tückisch, weil man sie so leicht übersieht. Sie kann provoziert werden durch die an sich gutgemeinte (vgl. 19.4.1) Einrichtung vieler Schlüsselnetze, wenn nicht äußerste Chiffrierdisziplin herrscht; sie entsteht auch als Folge kryptologischer Gedankenlosigkeit (Spruchschlüssel-Verdopplung bei der ENIGMA bis Mai 1940, vgl. 19.6.1). Spezifische Angriffsmethoden sind in 19.4 und 19.5

[5] Ihre Fähigkeiten können damit illustriert werden, daß ihr eines Tages auffiel, daß in einem ENIGMA-Chiffrat ein langer Teiltext kein L enthielt. Dies überhaupt zu bemerken, war unerhört. Sie zog aber auch den raffinierten Schluß, beim Klartext handle es sich um einen langen Füller mit lauter /l/, was sich bestätigte und zum Sieg der britischen Flotte über die italienische am 28. März 1941 bei Kap Matapán vor Griechenland beitrug.

diskutiert. Geheimtext-Geheimtext-Kompromittierung erlaubt reine Kryptanalyse und kann mit Supercomputern unterstützt werden.

Öffentliche Schlüssel tragen von vornherein die Möglichkeit einer Geheimtext-Geheimtext-Kompromittierung in sich und sollten dagegen gesichert sein.

22.2.5 Bei zusammengesetzten Verfahren versucht man, eine Chiffrierung nach der anderen abzustreifen. Dies ist besonders dann einfach, wenn über ein schon länger gebrauchtes, zwischenzeitlich gebrochenes Verfahren ein neues gelegt wird: Der Zwischentext ist dann als bekannte Sprache anzusehen; oder wenn ein schon länger gebrauchtes, zwischenzeitlich gebrochenes Verfahren als Überchiffrierung für eine neu eingeführte Chiffrierung benutzt wird (SD, 19.6.3.1). Überhaupt hätten die deutschen Dienste die Fähigkeiten des polnischen Büros, ihre ENIGMA zu brechen, gar nicht besser fördern können: Sie führten schrittweise neue Schikanen ein, die jedesmal zu spät kamen; so spät, daß die Polen wie die Briten nur jeweils einen Schritt bewältigen mußten.

Dies passierte auch bei anderen Gelegenheiten: Als im April 1944 Dokumente über ein ‚Reserve-Handschlüssel-Verfahren' auf Mykonos in feindliche Hände fielen, änderte man das Verfahren nicht gänzlich, sondern nur schrittweise und erzog so die Briten.

22.2.6 Nicht mehr ins Gebiet der reinen Kryptanalyse gehört die Beschaffung von gegnerischen Chiffrier- und Schlüsselunterlagen jeder Art bis hin zu ganzen Maschinen: durch illegalen Kauf, durch Ausspähung beim Zoll, durch Diebstahl und Einbruch, durch Kampfhandlungen (11.1.10). Die Erfahrungen des 2. Weltkriegs haben *Kerckhoffs* Mahnung und *Shannon*s Maxime „der Feind kennt das benutzte System" voll bestätigt. Die SIGABA (ECM Mark II) der U.S. Army war eines der wenigen Geräte des 2. Weltkriegs, das allem Anschein nach nicht in gegnerische Hände fiel, und dies wohl auch nur, weil nach der Landung in der Normandie der Krieg kein Jahr mehr dauerte.

Im übrigen dient auch die Zerstörung der leitungsgebundenen Nachrichtenverbindungen, wie sie die Alliierten vor und während der Landung in der Normandie betrieben, der Kryptanalyse; sie bewirkt *"to force a proportion of useful intelligence on to the air" (Ralph Bennett).*

22.2.7 Die wichtigste Waffe zur Abwehr der Kryptanalyse scheint die Phantasie zu sein. Man muß sich in die Denkart des unbefugten Entzifferers vollständig hineindenken können und man muß das auch noch wollen. Psychologisch begründete Hemmnisse und Wunschvorstellungen sind ebenso fehl am Platz wie arrogante Überheblichkeit. Drei Beispiele von folgenschwerer Gedankenlosigkeit seien aus dem Bereich der ENIGMA-Entzifferung angeführt:

1. Völlig unnötigerweise wurde anfangs bei der Luftwaffe nie der selbe Rotor in der selben Position an zwei aufeinanderfolgenden Tagen benutzt, und nie ein und die selbe Rotorenlage zweimal im selben Monat. Diese „scheinbare Zufälligkeit" sparte den Briten eine Menge Arbeit bei der Exhaustion der Rotorenlage, sobald erst eine unterbrechungsfreie Entzifferung gelungen war.

2. Völlig unnötigerweise durften niemals zwei aufeinanderfolgende Buchstaben, wie /a/ und /b/, durch Stecker verbunden werden. Das reduzierte die durchzuprüfenden Möglichkeiten für Steckerverbindungen und erlaubte den Briten sogar, eine eigene Fangschaltung dafür in die Bomben einzubauen, die sie witzigerweise CSKO, *'consecutive stecker knock-out'* nannten.

3. Völlig unnötigerweise war die Eingangs-Substitution (die durch das Steckerbrett bewirkt wurde) involutorisch. Weder bei der britischen TYPEX noch bei der japanischen PURPLE war diese ‚Vereinfachung' der Fall. Tatsächlich benutzten die Deutschen gelegentlich die ‚Uhr' (engl. *Uhr box*, Farbtafel M), einen unnatürlichen und plumpen Zusatz, der die Steckerbrett-Substitution[6] (nicht jedoch die ENIGMA-Chiffrierung) nicht-involutorisch machte, und einen häufigen Wechsel, vermutlich alle vollen Stunden, erlaubte — ein schlagender Beweis dafür, daß die deutsche Führung Bedenken wegen der Sicherheit der ENIGMA hatte, aber nicht mehr viel dagegen tun konnte.

Die kryptologische Abwehr muß nicht nur damit rechnen, daß der unbefugte Entzifferer viel Phantasie hat, sie muß selbst soviel Phantasie haben, daß sie sich die Phantasie des unbefugten Entzifferers vorstellen kann.

Die Fehler im Umfeld der ENIGMA nannte *Welchman* "*a comedy of errors.*" Er schrieb: "*The German errors ... stemmed from not exploring the theory of the Enigma cipher machine in sufficient depth, from weakness in machine operating procedures, message-handling procedures, and radio net procedures; and above all from failure to monitor all procedures.*" Spezifisch erwähnte er die Spruchschlüssel-Verdopplung, die '*Cillis*' und '*Herivel tips*', '*Parkerism*' (eine Angewohnheit der deutschen Hersteller von Chiffrierunterlagen, die 1942 in Blüte stand, ganze monatliche Sequenzen von Diskriminanten, Ringstellungen, Rotorlagen und Steckerverbindungen nach einiger Zeit zu wiederholen); und nicht zuletzt '*inadvertent assistance*' deutscher Stabsoffiziere bei der Bereitstellung von *cribs*. All diese Fehler können ausschließlich den Menschen angelastet werden, die sich der ENIGMA bedienten: "*the [ENIGMA] machine as it was would have been impregnable if it had been used properly.*"

22.3 Illusion der Sicherheit

Welchman könnte ironisch hinzugefügt haben, daß gerade dies nicht erwartet werden darf — im Einklang mit *Rohrbach*s Maxime (11.2.5) daß keine Maschine und kein Kryptosystem jemals die ganze Zeit fehlerfrei benutzt werden. Der im Krieg dienstverpflichtete Mathematiker Hans Rohrbach wußte das, und *Adolf Paschke*, Vortragender Legationsrat im Auswärtigen Amt und nomineller Chef der Sprachengruppe des Pers Z, wußte es ebenfalls.

[6] Die ‚Uhr' benutzt 10 Steckerpaare und hat 40 Positionen, von denen 10 (Nr. 00, 04, 08, ... 36) die Involution bewahren. Der eingebaute Vertauscher bewirkt eine Permutation mit der Zyklendarstellung (1 31 5 39 9 23 17 27 33 19 21 3 29 35 13 11) (0 6 16 26) (2 4 18 24) (12 38 32 22) (14 36 34 20) (7 25) (8 30) (10 28) (15 37).

Er lehnte strikt den Gebrauch der ENIGMA für diplomatische Kanäle ab, sogar für Gegenstände geringerer Bedeutung, wie Visaangelegenheiten. Chiffriermaschinen sah er scheel an, den Geheimschreiber T 52a betrachtete er als unsicher, tatsächlich fand man bei Paschke heraus, wie man den T 52a ohne viel Mühe brechen konnte. Das erklärt auch, warum *Beurling* keine unüberwindlichen Schwierigkeiten hatte. Und mit T 52e chiffrierte Nachrichten, die von Militärattachés über Kanäle des Auswärtigen Amtes geleitet wurden, wurden von den Leuten bei Pers Z übungshalber selbst gebrochen. Nur für nicht-geheime Nachrichten innerhalb Deutschlands über Drahtverbindungen wurde T 52 als annehmbar angesehen. Eine Ausnahme machte man ab 1944 auf der Funkverbindung zwischen Berlin und der Botschaft in Madrid, wobei für Nachrichten bis zur Klassifizierung 'Geheim' der Lorenz Schlüsselzusatz SZ 42 verwendet wurde, nicht aber für solche mit der Spitzenklassifikation 'Geheime Reichssache'. Darin spiegelt sich die Vorsicht wider, die Pers Z walten ließ.

Aber andernorts und anderswie blühte der Geist der illusionären Sicherheit. Wenn immer sich eine Gelegenheit fand für ein schnelleres und weniger sicheres kryptographisches Verfahren, hatte es gute Aussichten. Wunschdenken überwog. Abgesehen von den wenigen Fällen, wo individuelle Schlüssel überhaupt verwendet wurde, Zufallstests passierten und nur einmal gebraucht wurden, blieben nur sehr wenige kryptologische Systeme zwischen 1900 und 1950 ungebrochen. Im Falle der ENIGMA blieben zwar die Schlüsselnetze ‚Neptun', ‚Thetis', ‚Aegir', ‚Sleipnir' undurchdringbar, aber einige hatten nur wenig Verkehr oder wurden von den Alliierten als nicht bedeutsam genug angesehen.

Überwachung des eigenen Verkehrs wurde gelegentlich vorgenommen, beispielsweise wenn *Frank Rowlett* eine Schwachstelle herausfand in *Friedman*s Converter M-228 SIGCUM, der im Januar 1943 in Betrieb ging (8.8.6). Es hätte sich ausgezahlt, wenn beispielsweise im OKW eine Spezialgruppe den ENIGMA-Verkehr von Görings undisziplinierter Luftwaffe kontrolliert hätte; sie hätte die Löcher herausgefunden, von denen die Briten lebten, und hätte sie gestopft, um weiteres Unheil zu verhindern.

Aber selbst Überwachung hilft wenig, wenn sie unzulänglich vorgenommen wird. *Paschke* wußte selbstverständlich, daß die individuellen Schlüssel des AA mechanisch hergestellt wurden durch eine Anordnung von 48 fünfziffrig-zählenden Druckern; nach jedem Druckvorgang wurden die meisten dieser Zähler in einer als unregelmäßig angesehenen Weise weitergestellt ('komplementärer Antrieb'). Als besondere Vorsichtsmaßnahme galt, daß nacheinander gedruckte Bögen niemals in den selben Block gelegt wurden. Das schien vollkommen zu genügen, war aber unzureichend, wie die FLORADORA-Geschichte (8.8.7) beweist.

22.4 Kommunikationstheoretische Bedeutung der Kryptologie

Der Leser, der dieses Buch Kapitel für Kapitel las, mag es zunächst schwer gefunden haben, ein gelegentliches Lächeln zu unterdrücken. Die historische Kryptologie ist voller spannender, lustiger, anzüglicher Geschichten. Das macht sie selbst für den Laien so reizvoll.

Aber Schritt für Schritt ziehen ernste Schatten über die Geschichte der Kryptologie. Die Schlacht von Tannenberg im 1. Weltkrieg liefert ein Beispiel. Der Eintritt der U.S.A. in den fürchterlichen Krieg wurde ausgelöst durch die Entzifferung eines Telegramms mit Datum 16. Januar 1917 des deutschen Außenministers *Arthur Zimmermann* an seinen Botschafter in Mexiko, *Heinrich von Eckardt*, das in Londons *Room 40* der *Admiralty* von *Nigel de Grey* entziffert wurde. Sein Inhalt – Mexiko aufzustacheln gegen seinen nördlichen Nachbarn – wurde dem Präsidenten *Woodrow Wilson* zugespielt, der zu dem Schluß kam, daß "*right is more precious than peace.*" Und die Ereignisse aus dem 2. Weltkrieg spielen vor einem Hintergrund des Grauens.

Die Zeit des Kalten Krieges hat ebenfalls ihre menschenverachtenden Züge gezeigt, die zwar durch Spionageromane verniedlicht wurden, aber nicht zu vergessen sind.

Im Gespräch mit einem Angehörigen hoheitlicher Dienste ist immer Vorsicht und Taktgefühl am Platze. Manchmal tritt einem die Überlegenheit des Professionellen gegenüber, der zwar zeigt, daß er etwas weiß, aber nicht, was er weiß. Sich bedeckt zu halten, dazu besteht Grund, wie das Beispiel *Welchman* zeigt, der sich nach der Veröffentlichung seines Buches 'The Hut Six Story' Angriffen ausgesetzt sah.

22.4.1 Kryptanalyse wurde von vielen Beteiligten als schwere Last empfunden; nicht so sehr der Nervenbelastung wegen, sondern unter dem Druck des Gewissens. Diese Beschwernis teilt aber die Kryptologie nicht nur mit anderen Zweigen der Mathematik und der Informatik, die dem Mißbrauch offenstehen, sondern ganz besonders mit naturwissenschaftlichen Disziplinen wie Physik, Chemie und Biologie – es wird genügen, als Stichwörter *Kernenergie, Giftgas, Genmanipulation* zu nennen. Der Preis, den unser Jahrhundert für die enormen Fortschritte der Wissenschaft – die ja niemand missen möchte – bezahlt, wird auch den Forschern selbst abverlangt: Sie müssen sich hohen Anforderungen an Menschlichkeit gewachsen zeigen. Der Zusammenbruch einiger kommunistischer Unrechtssysteme und die wachsende Betroffenheit der Menschen über ihre unbegrenzten Möglichkeiten läßt hoffen, daß die Forscher Einsicht und Zurückhaltung zeigen werden.

Die Kryptologie braucht also ebensowenig wie die Naturwissenschaften verteufelt zu werden. Mit einer positiven Sicht sagen *Meyer* und *Matyas*:

> *"Cryptography is the only known practical means for protecting information transmitted through large communication networks such as telephone lines, microwave, or satellite."*

und anderswo ist zu lesen

> *"Cryptology has metamorphosized from an arcane art to a respectable subdiscipline of Computer Science."*

Die Folklore drückt es auch so aus

> *"Today, code-making and code-breaking are games anybody can play."*

Tatsächlich finden sich heute wissenschaftliche Originalbeiträge kryptologischer Natur nicht nur in den (wenigen) Spezialzeitschriften und -symposien, sondern in der gesamten Informatik, insbesondere in der Theoretischen Informatik. Berührungen und gegenseitige Befruchtungen gibt es insbesondere mit der rasch aufstrebenden Komplexitätstheorie, mit der Theorie der formalen Sprachen, und selbstverständlich weiterhin in der Mathematik mit der Zahlentheorie und der Kombinatorik.

22.4.2 Aber auch in der Kryptologie selbst sind mit der Informationstheorie von *Shannon* und *Rényi* neue Inhalte hinzugekommen, und mit den *public keys* neue Denkweisen zwar nicht erst entstanden, aber in den Vordergrund getreten, wie etwa asymmetrische Chiffrierverfahren und Authentisierung. Letzteres Problem führt über die bloße Geheimhaltungstendenz hinaus auf allgemeine Gesichtspunkte der Kommunikation: Wird als **Protokoll** das verabredete Verfahren der Kommunikation bezeichnet, so schließt ein kryptographisches Protokoll zwischen zwei Partnern Maßnahmen ein, die nicht nur vom Mißtrauen gegenüber allen Dritten getragen sind, sondern auch vom teilweisen Mißtrauen untereinander. Das Problem mag sein, wie die Partner gewisse Geheimnisse teilen können, ohne dadurch andere Geheimnisse preiszugeben. Das Problem mag auch sein, wie die Partner Schritt für Schritt Vertrauen aufbauen, ohne dabei Risiken des Geheimnisverlusts einzugehen. Anwendungen auf das gegenseitige Verhalten von Großmächten, von Parteien, von Firmengruppen liegen auf der Hand. Als einfache und mehr alltägliche Beispiele mögen dienen: Der Vorgang des Nachweises eines Scheckkarteninhabers gegenüber einer Bank (oder einem Bankautomaten), daß er der Eigentümer (und damit der rechtmäßige Besitzer) ist, oder eine Lizenzverhandlung, bei der der Erfinder den präsumtiven Lizenznehmer von der Brauchbarkeit und Wirksamkeit seines Verfahrens überzeugen muß, ohne dieses vor Vertragsabschluß preiszugeben (**gedeckter Beweis**, *engl. Zero-Knowledge Proof*): Der präsumtive Lizenznehmer erfährt vom Erfinder nichts, was er nicht selbst herausfinden könnte.

Das Problem ist alt: Schon zu den Zeiten von *Tartaglia* und *Cardano* wußten Mathematiker ihre algebraischen Verfahren geheimzuhalten und nur Stück für Stück auf einzelne ihnen gestellte Probleme demonstrativ anzuwenden, prototypisch bei der Lösung von algebraischen Gleichungen durch Radikale. Wie man weiß, gelang es *Cardano* trotzdem, *Tartaglia* sein Verfahren für Gleichungen dritten Grades abzulisten. Der arme *Niccolò Tartaglia* hat unsere volle Sympathie.

22.4.3 Die Kryptanalyse im weitesten Sinn greift über den in diesem Buch geschilderten Rahmen hinaus. Die Erforschung der Natur ist oft eine Entzifferung ihrer Geheimnisse.

Beispielsweise ist die Röntgen-Strukturanalyse von Proteinen eine kryptanalytische Aufgabe: Zu bestimmen ist die Phasenlage, die zu einer gemessenen Amplitudenfunktion der Frequenzen im Röntgen-Beugungsbild gehört. Nur wenn Phasenlage (der zu findende Schlüssel) und Amplitudenfunktion (der Geheimtext) so zusammenpassen, daß sie eine physikalische Realität (den Klartext) mit positiver Elektronendichte und der richtigen Anzahl von Atomen ergeben, ist die Entzifferung gelungen. Dabei spielen Annahmen über den Molekülaufbau – etwa die Struktur der Doppelwendel der DNA, die *Watson* und *Crick* vermuteten – die Rolle wahrscheinlicher Wörter im Klartext. Auf diese Sicht haben schon in den fünfziger Jahren *Alan Turing* und *David Sayre* hingewiesen.

Das Auffinden einer Nadel im Heuhaufen bei der Suche nach Elementarteilchen ist noch keine kryptanalytische Aufgabe, eher schon die von *Norbert Wiener* behandelte Glättung (*smoothing*) von Signalen, insbesondere das Abstreifen des Rauschens über einem Signal, wie es bei Übertragungen von und zu Weltraumfahrzeugen erforderlich ist. Das Auffinden von Mustern irgendeiner, bisher *völlig unbekannten* Art ist jedoch Kryptanalyse und kann sich deren fortgeschrittenen Methoden bedienen, etwa der *Friedman*schen Koinzidenz-Untersuchung (Kullback-Entropie) oder des im *Turing*schen *banburism* verwendeten *weight of evidence* (Shannon-Entropie). Generell ist die Rolle, die die Renyi-Entropie und die im Anhang skizzierte Axiomatische Informationstheorie dabei spielen kann, noch zu erforschen.

Und da ist schließlich die Hauptaufgabe des denkenden Menschen: Das Erkennen von Situationen, das Bilden von Begriffen, das Gewinnen der Abstraktion. Das ist im weitesten Sinn eine kryptanalytische Aufgabe: Es gilt, etwas Verborgenes, etwas im Verborgenen bereits Existierendes herauszufinden. Es gilt, zwischen den Zeilen zu lesen, Intelligenz zu zeigen. *Pure Cryptanalysis* versucht das ohne Zutun von Intuition, ihr entspricht die schlagwortartige *Artificial Intelligence*, die, so weit sie reicht, auch nicht zu beanstanden ist. Das breite Instrumentarium der Kryptanalyse nutzt jedoch, wie dieses Buch gezeigt haben sollte, die Intuition, und das mit List und Schläue.

Die Kryptanalyse kann also auch als Vorbild für die Methodik anderer Wissenschaften dienen. In diesem Sinne ist dieses Buch geschrieben. *Babbage* schrieb (“*Passages from the Life of a Philosopher*”)

> *“Deciphering is, in my opinion, one of the most fascinating of arts, and I fear I have wasted upon it more time than it deserves.”*

Ich habe dabei keine Mühe gescheut, aber hoffentlich doch keine Zeit verschwendet.

A Anhang: Perfekte Sicherheit und praktische Sicherheit

"The logic of secrecy was the mirror-image of the logic of information"

Colin Burke, 1994

Perfekte Sicherheit wurde seit jeher gerne von den Erfindern von Chiffriersystemen, im besonderen von Chiffriermaschinen, versprochen (*Bazeries*: *je suis indéchiffrable*, 2.1.1 Abb. 19). Jedoch gab erst 1949 *Claude E. Shannon* eine saubere Definition davon, was mit perfekter Sicherheit gemeint sei; er gab sie im allgemeinen Rahmen seiner Informationstheorie.[1] Da der wahrscheinlichkeitstheoretische Apparat, den sie benutzt, außerhalb des Rahmens dieses Buches liegt, geben wir nur eine verkürzte, dafür aber axiomatische Übersicht.

A.1 Axiome einer axiomatischen Informationstheorie

Man geht zweckmäßigerweise aus von der **Unsicherheit** (engl. *uncertainty, equivocation*) über eine Menge $\mathcal{X}$ von Ereignissen, der „Entropie" von $\mathcal{X}$ — eine reelle Zahl . Auch $\mathcal{Y}$ und $\mathcal{Z}$ seien Mengen von Ereignissen.

$H_{\mathcal{Y}}(\mathcal{X})$ bezeichne die Unsicherheit über $\mathcal{X}$, falls $\mathcal{Y}$ bekannt ist.

A.1.1 Intuitiv einleuchtende Axiome für die zweistellige Mengenfunktion H sind:

(0) $0 \leq H_{\mathcal{Y}}(\mathcal{X})$ („Unsicherheit ist nichtnegativ")

Für $0 = H_{\mathcal{Y}}(\mathcal{X})$ sagen wir "$\mathcal{Y}$ bestimmt eindeutig $\mathcal{X}$."

(1) $H_{\mathcal{Y}\cup\mathcal{Z}}(\mathcal{X}) \leq H_{\mathcal{Z}}(\mathcal{X})$ („Unsicherheit nimmt nicht zu, wenn mehr bekannt")

Für $H_{\mathcal{Y}\cup\mathcal{Z}}(\mathcal{X}) = H_{\mathcal{Z}}(\mathcal{X})$ sagen wir "$\mathcal{Y}$ sagt nichts aus über $\mathcal{X}$."

Von entscheidender Bedeutung ist das Axiom

(2) $H_{\mathcal{Z}}(\mathcal{X} \cup \mathcal{Y}) = H_{\mathcal{Y}\cup\mathcal{Z}}(\mathcal{X}) + H_{\mathcal{Z}}(\mathcal{Y})$.

(„Unsicherheit kann additiv über der Vereinigung von Ereignissen aufgebaut werden").

---

[1] *Shannon* hatte frühzeitig Berührung mit der Kryptanalyse; er arbeitete 1936-1938 im Team von *Vannevar Bush*, der den COMPARATOR zur Bestimmung der Zeichen-Koinzidenz entwickelte. Seine bis 1940 zurückreichende Arbeit in den Bell Laboratories (vgl. 16.5) führte zu einem vertraulichen Bericht (A Mathematical Theory of Communication) vom 1. Sept. 1945, der neben der Definition der Shannon-Entropie (16.5) die nachfolgend erörterten Grundbeziehungen enthält (publiziert 1949: Communication Theory of Secrecy Systems, Bell System Technical Journal 28, 656-715 (1949).

(Das übliche stochastische Modell für diese axiomatische Informationstheorie geht aus von $p_X(a) = \Pr[X = a]$, der Wahrscheinlichkeit, daß die Zufallsvariable X den Wert a annimmt, und definiert

$$H_\emptyset(\{X\}) = - \sum_{s\,:\,p_X(s)>0} p_X(s) \cdot \mathrm{ld}\, p_X(s)$$

$$H_\emptyset(\{X\} \cup \{Y\}) = - \sum_{s,t\,:\,p_{X,Y}(s,t)>0} p_{X,Y}(s,t) \cdot \mathrm{ld}\, p_{X,Y}(s,t)$$

$$H_{\{Y\}}(\{X\}) = - \sum_{s,t:\ p_{X/Y}(s/t)>0} p_{X,Y}(s,t) \cdot \mathrm{ld}\, p_{X/Y}(s/t)$$

wobei $p_{X,Y}(a,b) =_{\text{def}} \Pr[(X = a) \wedge (Y = b)]$ und $p_{X/Y}(a/b)$ der Bayesschen Regel für bedingte Wahrscheinlichkeiten genügt:

$$p_{X,Y}(s,t) = p_Y(t) \cdot p_{X/Y}(s/t) \quad \text{, also}$$

$$-\mathrm{ld}\, p_{X,Y}(s,t) = -\mathrm{ld}\, p_Y(t) - \mathrm{ld}\, p_{X/Y}(s/t) \ \ .\,)$$

A.1.2 Aus (0), (1) und (2) können all die anderen Eigenschaften erhalten werden, die für das klassischerweise übliche stochastische Modell gelten.

Aus (2) ergibt sich mit $\mathcal{Y} = \emptyset$

(2a) $H_\mathcal{Z}(\emptyset) = 0$ („Über die leere Ereignismenge gibt es keine Unsicherheit“)

Aus (1) und (2) ergibt sich beispielsweise

(3a) $H_\mathcal{Z}(\mathcal{X} \cup \mathcal{Y}) \leq H_\mathcal{Z}(\mathcal{X}) + H_\mathcal{Z}(\mathcal{Y})$ („Unsicherheit ist subadditiv“)

Aus (0) und (2) ergibt sich überdies

(3b) $H_\mathcal{Z}(\mathcal{Y}) \leq H_\mathcal{Z}(\mathcal{X} \cup \mathcal{Y})$ („Unsicherheit wächst mit Ereignismenge“)

Unter Benutzung der Kommutativität von $. \cup .$ erhält man aus (2)

(4) $H_\mathcal{Z}(\mathcal{X}) - H_{\mathcal{Y}\cup\mathcal{Z}}(\mathcal{X}) = H_\mathcal{Z}(\mathcal{Y}) - H_{\mathcal{X}\cup\mathcal{Z}}(\mathcal{Y})$

(„$\mathcal{Y}$ sagt nichts über $\mathcal{X}$ aus“ und „$\mathcal{X}$ sagt nichts über $\mathcal{Y}$ aus“ sind gleichwertig)

(4) legt folgende Definition nahe: Die **gegenseitige Information** (‘*mutual information*’) von $\mathcal{X}$ und $\mathcal{Y}$ bei Kenntnis von $\mathcal{Z}$ ist definiert als

$$I_\mathcal{Z}(\mathcal{X}, \mathcal{Y}) =_{\text{def}} H_\mathcal{Z}(\mathcal{X}) - H_{\mathcal{Y}\cup\mathcal{Z}}(\mathcal{X}) \ .$$

Die Information $I_\mathcal{Z}(\mathcal{X}, \mathcal{Y})$ ist somit eine symmetrische und wegen (1) nichtnegative Funktion der Ereignismengen $\mathcal{X}$ und $\mathcal{Y}$. Es ist wegen (2)

$$I_\mathcal{Z}(\mathcal{X}, \mathcal{Y}) = H_\mathcal{Z}(\mathcal{X}) + H_\mathcal{Z}(\mathcal{Y}) - H_\mathcal{Z}(\mathcal{X} \cup \mathcal{Y}) \ .$$

$I_\mathcal{Z}(\mathcal{X}, \mathcal{Y}) = 0$ besagt, daß $H_{\mathcal{Y}\cup\mathcal{Z}}(\mathcal{X}) = H_\mathcal{Z}(\mathcal{X})$ und $H_{\mathcal{X}\cup\mathcal{Z}}(\mathcal{Y}) = H_\mathcal{Z}(\mathcal{Y})$ ist. Dafür sagt man auch, daß „bei Kenntnis von $\mathcal{Z}$ $\mathcal{Y}$ nichts über $\mathcal{X}$ aussagt und $\mathcal{X}$ nichts über $\mathcal{Y}$, daß also $\mathcal{X}$ und $\mathcal{Y}$ **gegenseitig unabhängig** sind“.

(Im üblichen stochastischen Modell liegt diese Situation gerade dann vor, wenn X, Y unabhängige Zufallsvariable sind: $p_{X,Y}(s,t) = p_X(s) \cdot p_Y(t)$.)

$I_\mathcal{Z}(\mathcal{X}, \mathcal{Y}) = 0$ ist gleichwertig mit der Additivität von H:

(5) $I_\mathcal{Z}(\mathcal{X}, \mathcal{Y}) = 0$ genau dann, wenn $H_\mathcal{Z}(\mathcal{X}) + H_\mathcal{Z}(\mathcal{Y}) = H_\mathcal{Z}(\mathcal{X} \cup \mathcal{Y})$.

A.2 Informationstheorie von Chiffrierungen

Für eine Chiffrierung **X** seien Ereignisse im Sinne der abstrakten Informationstheorie Mengen von endlichen Texten, über Z_m als Alphabet. Es sei P ein Klartext-, C ein Geheimtext-, K ein Schlüssel-Ereignis.[2]

A.2.1 Für die Unsicherheiten (*equivocations*)

$H(K),\ H_C(K),\ H_P(K),\ H(C),\ H_P(C),\ H_K(C),\ H(P),\ H_K(P),\ H_C(P)$ erhält man aus (1), invariant gegen zyklische Vertauschung von P, C, K:

$$\begin{aligned} H(K) &\geq H_P(K)\ , & H(C) &\geq H_P(C)\ , \\ H(C) &\geq H_K(C)\ , & H(P) &\geq H_K(P)\ , \\ H(P) &\geq H_C(P)\ , & H(K) &\geq H_C(K)\ . \end{aligned}$$

A.2.1.1 Ist **X** funktional, so ist C durch P und K eindeutig bestimmt:

(CHIFF) $H_{P,K}(C) = 0$ d.h. $I_K(P,C) = H_K(C)$, $I_P(K,C) = H_P(C)$

(„Klartext und Schlüssel zusammen lassen keine Unsicherheit über den Geheimtext zu").

A.2.1.2 Ist **X** injektiv, so ist P durch C und K eindeutig bestimmt:

(DECHIFF) $H_{C,K}(P) = 0$ d.h. $I_K(P,C) = H_K(P)$, $I_C(K,P) = H_C(P)$

(„Geheimtext und Schlüssel zusammen lassen keine Unsicherheit über den Klartext zu").

A.2.1.3 Ist **X** eine *Shannonsche* Chiffrierung, so ist auch der Schlüssel K durch Klartext P und Geheimtext C eindeutig bestimmt:

(SHANN) $H_{P,C}(K) = 0$ d.h. $I_P(K,C) = H_P(K)$, $I_C(K,P) = H_C(K)$

(„Klartext und Geheimtext zusammen lassen keine Unsicherheit über den Schlüssel zu").

A.2.2 Aus (4) folgt sofort

$$\begin{aligned} H_K(C) + H_{K,C}(P) &= H_K(P) + H_{P,K}(C)\,, \\ H_P(C) + H_{P,C}(K) &= H_P(K) + H_{P,K}(C)\,, \\ H_K(P) + H_{K,P}(C) &= H_K(C) + H_{C,K}(P)\,, \\ H_C(P) + H_{C,P}(K) &= H_C(K) + H_{C,K}(P)\,, \\ H_P(K) + H_{P,K}(C) &= H_P(C) + H_{P,C}(K)\,, \\ H_C(K) + H_{C,K}(P) &= H_C(P) + H_{P,C}(K)\ . \end{aligned}$$

Mit (1) erhält man daraus

Satz 1:

(CHIFF)	impliziert	$H_K(C) \leq H_K(P)$, $H_P(C) \leq H_P(K)$,
(DECHIFF)	impliziert	$H_K(P) \leq H_K(C)$, $H_C(P) \leq H_C(K)$,
(SHANN)	impliziert	$H_P(K) \leq H_P(C)$, $H_C(K) \leq H_C(P)$.

[2] Einem weitverbreiteten notationellen Mißbrauch folgend, ersetzen wir im folgenden $\{X\}$ durch X und $\{X\} \cup \{Y\}$ durch X, Y ; auch lassen wir $\emptyset$ als Subskript weg.

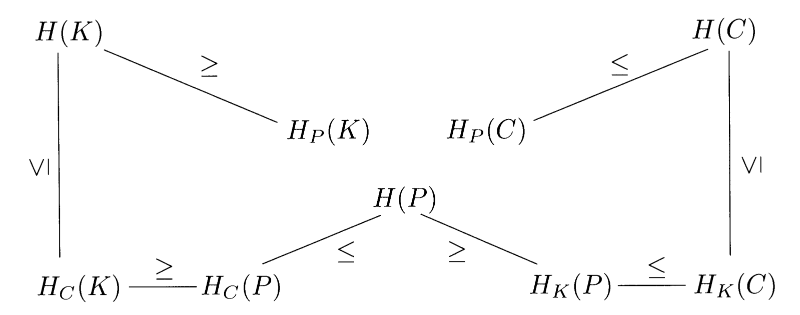


Abb. 163. Relationen zwischen Unsicherheiten für injektive Chiffrierungen

Chiffrierungen sind normalerweise injektiv, (DECHIFF) gilt. Aus Abb. 163 sind graphisch die daraus resultierenden numerischen Relationen zwischen den Unsicherheiten zu ersehen.

A.2.3 Die Konjunktion von irgendwelchen zwei der drei Bedingungen (CHIFF), (DECHIFF), (SHANN) führt wegen der Antisymmetrie der Kleiner-Gleich-Relation zu Gleichheiten:

Satz 2:

(CHIFF) $\wedge$ (DECHIFF) impliziert $H_K(P) = H_K(C)$,

(DECHIFF) $\wedge$ (SHANN) impliziert $H_C(P) = H_C(K)$,

(CHIFF) $\wedge$ (SHANN) impliziert $H_P(C) = H_P(K)$.

In einer *klassischen* Chiffrierung, d.h. einer ohne Homophone und Polyphone, gelten (CHIFF) und (DECHIFF), also

> „Die Unsicherheit über den Geheimtext bei Kenntnis des Schlüssels ist gleich der Unsicherheit über den Klartext bei Kenntnis des Schlüssels“.

In vielen professionellen Chiffrierungen gilt (vgl. 2.6.4) die Shannon-Bedingung (SHANN). In einer *klassischen Shannonschen* Chiffrierung gelten alle drei Gleichheiten (Abb. 164). Monoalphabetische einfache Substitution und Transposition sind triviale, VIGENÈRE, BEAUFORT und VERNAM sind ernsthafte Beispiele solcher klassischen Shannonschen Chiffrierungen.

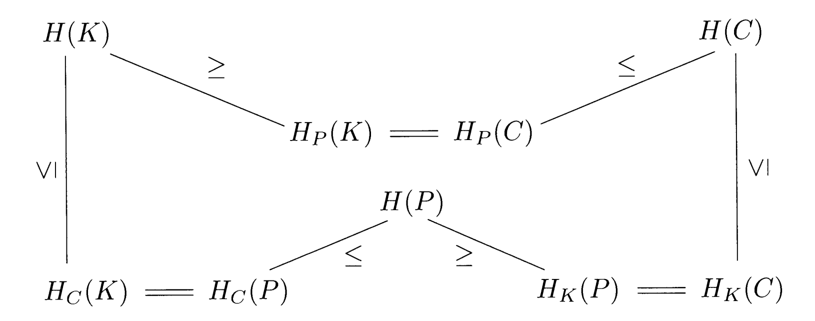


Abb. 164. Relationen zwischen Unsicherheiten für klassische Shannonsche Chiffrierungen

A.3 Perfekte und individuelle Chiffrierungen

A.3.1 Eine Chiffrierung **X** soll **perfekt** heißen, wenn Klartext und Geheimtext gegenseitig unabhängig sind:

$$I(P,C) = 0 \ .$$

Dies ist äquivalent zu $H(P) = H_C(P)$ und zu $H(C) = H_P(C)$

(„Ohne Kenntnis des Schlüssels ändert die Kenntnis des Geheimtextes nichts an der Unsicherheit über den Klartext, und die Kenntnis des Klartextes nichts an der Unsicherheit über den Geheimtext"),

wie auch nach (5) äquivalent zu $H(P,C) = H(P) + H(C)$.

Satz 3^K: (*Shannon*s pessimistische Ungleichung)
In einer perfekten *klassischen* Chiffrierung gilt

$$H(P) \leq H_C(K) \leq H(K) \quad \text{und} \quad H(C) \leq H_P(K) \leq H(K) \ .$$

Bew.: $H(P) = H_C(P)$ (*ist perfekt*)
$H_C(P) \leq H_C(K)$ (DECHIFF), Satz 1
$H_C(K) \leq H(K)$ (1) .

Analog mit (CHIFF) und Satz 1 für $H(C)$. ⋈

In einer perfekten klassischen Chiffrierung ist also die Unsicherheit über den Schlüssel nicht kleiner als die Unsicherheit über den Klartext sowie nicht kleiner als die Unsicherheit über den Geheimtext.

A.3.2 Eine Chiffrierung **X** soll **Chiffrierung mit individuellem Einmal-Schlüssel**, kurz **individuelle Chiffrierung** heißen, wenn Klartext und Schlüssel gegenseitig unabhängig sind:

$$I(K,P) = 0 \ .$$

Dies ist äquivalent zu $H(K) = H_P(K)$ und zu $H(P) = H_K(P)$

(„Ohne Kenntnis des Geheimtexts ändert die Kenntnis des Schlüssels nichts an der Unsicherheit über den Klartext, und die Kenntnis des Schlüssels nichts an der Unsicherheit über den Klartext"),

wie auch nach (5) äquivalent zu $H(K,P) = H(K) + H(P)$.

Satz 3^C:
In einer individuellen Shannonschen Chiffrierung gilt

$$H(K) \leq H_P(C) \leq H(C) \quad \text{und} \quad H(P) \leq H_K(C) \leq H(C) \ .$$

Bew.: $H(K) = H_P(K)$ (*ist individuell*)
$H_P(K) \leq H_P(C)$ (SHANN), Satz 1
$H_P(C) \leq H(C)$ (1) .

Analog mit (DECHIFF) und Satz 1 für $H(P)$. ⋈

In einer individuellen Shannonschen Chiffrierung ist also die Unsicherheit über den Schlüssel wie auch über den Klartext kleiner oder gleich der Unsicherheit über den Geheimtext.

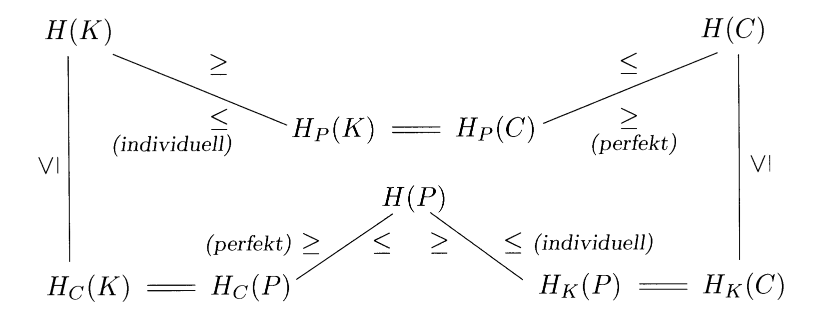


Abb. 165. Relationen zwischen Unsicherheiten für klassische Shannonsche Chiffrierungen mit den Eigenschaften *perfekt* und *individuell*

A.3.2 In einer klassischen Shannonschen Chiffrierung gilt noch mehr: Aus den Relationen in Abb. 165 und speziell in Abb. 166 sieht man sofort

Satz 4 :
In einer klassischen Shannonschen Chiffrierung, die perfekt ist, gelten

$$H(P) = H_C(P) = H_C(K) \quad \text{und} \quad H(C) = H_P(C) = H_P(K) \ ,$$
$$H(K) \geq H(C) \quad \text{sowie} \quad H(P) - (H(K) - H(C)) = H_K(C) = H_K(P) \ .$$

In einer individuellen klassischen Shannonschen Chiffrierung gelten

$$H(K) = H_P(K) = H_P(C) \quad \text{und} \quad H(P) = H_K(P) = H_K(C) \ ,$$
$$H(C) \geq H(K) \quad \text{sowie} \quad H(P) - (H(C) - H(K)) = H_C(K) = H_C(P) \ .$$

Bew.: Mit (DECHIFF) und (SHANN) folgt aus Satz 2 $H_C(P) = H_C(K)$ und somit nach beidseitiger Addition von $H(C)$ gemäß (2) $H(P,C) = H(K,C)$.
In einer perfekten Chiffrierung ist (A.3.1) $H(P,C) = H(P) + H(C)$;
mit (2) erhält man $H(K,C) = H(K) + H_K(C)$,
also $H_K(C) = H(P) - (H(K) - H(C))$.
Ähnlich folgt mit (CHIFF) und (SHANN) aus Satz 2 $H_P(K) = H_P(C)$ und nach beidseitiger Addition von $H(P)$ gemäß (2) $H(P,C) = H(K,P)$.
In einer individuellen Chiffrierung ist $H(K,P) = H(K) + H(P)$;
mit (2) erhält man $H(P,C) = H(C) + H_C(P)$,
also $H_C(P) = H(C) - (H(K) - H(P))$.

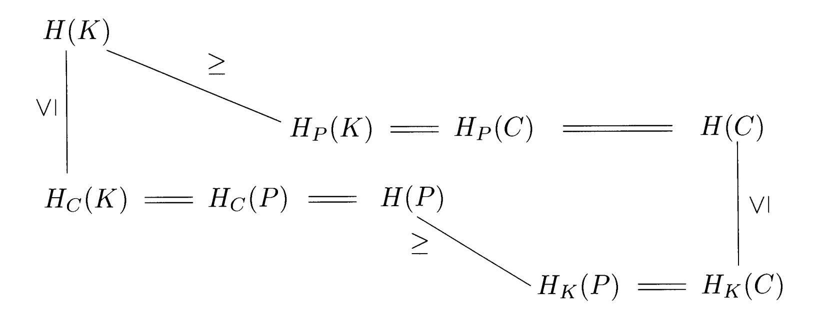


Abb. 166. Relationen zwischen Unsicherheiten für perfekte klassische Shannonsche Chiffrierungen

A.4 Shannonscher Hauptsatz

A.4.1 Für eine klassische Shannonsche Chiffrierung, die perfekt und individuell ist, gilt nach Satz 3 (s. auch Abb. 165) $H(K) = H(C)$.

A.4.2 Eine Chiffrierung soll **vom Vernamschen Typ** heißen, wenn

$$H(K) = H(C) \ .$$

(Im stochastischen Modell ist diese Bedingung insbesondere erfüllt, wenn C und K Texte von k Zeichen mit maximalem $H(K)$ und maximalem $H(C)$ sind: $H(K)=H(C)=k \cdot \mathrm{ld}\, N$

Beispiele liefern VIGENÈRE, BEAUFORT und speziell VERNAM, desgleichen lineare polygraphische Blockchiffrierungen mit geeigneten Schlüsseln.

Shannonscher Hauptsatz (*Claude E. Shannon 1949*):

In einer klassischen Shannonschen Chiffrierung ziehen je zwei der drei Eigenschaften *ist perfekt*, *ist individuell*, *ist vom Vernamschen Typ*
die dritte nach sich. Der Beweis ist offensichtlich aus Abb. 165.

A.4.3 Um einer klassischen Shannonschen Chiffrierung perfekte Sicherheit zu geben, ist es also hinreichend, daß es vom Vernamschen Typ ist und daß der Schlüssel individuell ist; beides sind Bedingungen, die von außen gewährleistet werden können. Nach Satz 3 gilt dann $H(P) \le H(K) = H(C)$.

(Im stochastischen Modell verlangt aber diese perfekte Sicherheit, daß eine sichere Verteilung eines Schlüssels gewährleistet ist, der für jedes Zeichen des Klartexts ein Schlüsselzeichen bereitstellt – eine extreme Forderung, die unter praktischen Gesichtspunkten oft nicht erfüllbar ist.[3] Praktische Sicherheit, die nicht perfekt ist, ist nur durch den Zeitaufwand, den das Brechen erfordert, gewährleistet.

A.4.4 *Shannon* diskutiert eine weitere Eigenschaft einer Chiffrierung; er nennt eine Chiffrierung **ideal** (*'strongly ideal'*), wenn Geheimtext und Schlüssel gegenseitig unabhängig sind:

$$I(K, C) = 0 \ .$$

Dies ist äquivalent zu $H(K) = H_C(K)$ und zu $H(C) = H_K(C)$.

Nach *Shannon* haben ideale Chiffrierungen praktische Nachteile: Damit eine ideale Chiffrierung auch perfekt ist, muß $H(K) = H(P)$ sein. Ideale Chiffrierungen müssen also genau der Klartextsprache, also meistens einer natürlichen Sprache, angepaßt werden. Dies erfordert ziemlich komplizierte Chiffriermechanismen bzw. Schlüsselerzeuger. Auch ist bei Übertragungsfehlern ein Lawineneffekt unvermeidlich. Es handelt sich also um ein praktisch unerreichbares Ideal.

---

[3] Perfekte Sicherheit verlangt also mit $H(P) \le H(K)$, daß im Modell der Schlüssel mindestens so viele Zeichen enthält als der Klartext, daß also auch jede Beschreibung des Schlüssels mindestens so lang ist wie der Schlüsssel — vgl. *Chaitin*s Forderung, 8.6.2.

A.5 Unizitätslänge und Codekomprimierung

Die Bedingung $H_C(P) > 0$ besagt, daß über den Klartext bei bekanntem Geheimtext noch eine Unsicherheit herrscht. Für eine Shannonsche Chiffrierung mit individuellem Schlüssel (die aber nicht perfekt zu sein braucht) bedeutet das nach Satz 4^C

$$H(K) > H(C) - H(P).$$

A.5.1 Wir gehen nun zum stochastischen Modell über, mit Klartextwörtern V^* und Geheimtextwörtern W^* über einem Zeichenvorrat $V = W$ von N Zeichen. Ferner beschränken wir uns auf Wörter der Länge k .

Wir nehmen (*Hellman* 1975) an, daß N_P und N_C Zahlen sind derart, daß unter den N^k Wörtern der Länge k die Anzahl der sinnvollen, d.h. vorkommenden Klartexte gerade $(N_P)^k$ und die Anzahl der vorkommenden Geheimtexte gerade $(N_C)^k$ beträgt. Es ist dann $N_P \leq N$ und $N_C \leq N$. Wenn alle diese Texte gleich häufig vorkommen, ist im stochastischen Modell

$$H(P) = k \cdot \operatorname{ld} N_P \ , \quad H(C) = k \cdot \operatorname{ld} N_C \ .$$

Des weiteren sei, wie in Kap. 12, Z die Mächtigkeit der Verfahrensklasse, also die Anzahl der Schlüsselwörter. All diese Schlüsselwörter sollen gleich häufig vorkommen. Dann ist

$$H(K) = \operatorname{ld} Z \ .$$

Die Ungleichung oben wird

$$\operatorname{ld} Z > k \cdot (\operatorname{ld} N_C - \operatorname{ld} N_P)$$

oder, falls $\operatorname{ld} N_C > \operatorname{ld} N_P$

$$k < U, \quad \text{wo} \quad U = \frac{1}{\operatorname{ld} N_C - \operatorname{ld} N_P} \cdot \operatorname{ld} Z \ .$$

Falls also, wie oben angenommen, eine Unsicherheit herrscht, ist $k < U$; ist somit $k \geq U$, so herrscht keine Unsicherheit. U ist also (vgl. 12.6) die Unizitätslänge.

Ist N_C maximal, $N_C = N$, kommen also alle *möglichen* Geheimtexte auch gleich häufig vor, so ist sicher die Bedingung $\operatorname{ld} N_C \geq \operatorname{ld} N_P$ erfüllt. Die Unizitätslänge beträgt dann, falls wie üblich $N_P < N$,

$$U = \frac{1}{\operatorname{ld} N - \operatorname{ld} N_P} \cdot \operatorname{ld} Z \ .$$

und wird somit durch den Wert von N_P für die Klartextwörter bestimmt. Dieser hängt aber von der im kryptanalytischen Verfahren vorgenommenen Analyse ab. Werden zur Analyse lediglich Einzelzeichenhäufigkeiten herangezogen, so ist auch $N_P = N_P^{(1)}$ bezüglich der Einzelzeichenhäufigkeiten zu betrachten; die Werte für $\operatorname{ld} N_P^{(1)}$ unterscheiden sich im Deutschen und im Englischen nicht sehr und betragen für die in 15.5 betrachtete Textbasis *SZ3* $\operatorname{ld} N_P^{(1)} \approx 4.07\,[\text{bit}]$, für die Auszählung Meyer-Matyas $\operatorname{ld} N_P^{(1)} \approx 4.17\,[\text{bit}]$, wobei $N = 26$ und $\operatorname{ld} N = \operatorname{ld} 26 \approx 4.70\,[\text{bit}]$.

Wenn wir also den mittleren Wert $\mathrm{ld}\, N_P^{(1)} \approx 4.1$ [bit] wählen und wenn wir weiterhin mit $\mathrm{ld}\, N_P^{(2)} \approx 3.5$ [bit] für Bigrammhäufigkeiten, $\mathrm{ld}\, N_P^{(3)} \approx 3.2$ [bit] für Trigrammhäufigkeiten rechnen, so ergeben sich die Unizitätslängen

(1) $U \approx \frac{1}{0.6}\, \mathrm{ld}\, Z$ für Entzifferung mittels Einzelzeichenhäufigkeiten,

(2) $U \approx \frac{1}{1.2}\, \mathrm{ld}\, Z$ für Entzifferung mittels Bigrammhäufigkeiten,

(3) $U \approx \frac{1}{1.5}\, \mathrm{ld}\, Z$ für Entzifferung mittels Trigrammhäufigkeiten.

Für Klartextwörter beträgt die mittlere Länge etwa 4.5 und die zugehörige Shannon-Entropie etwa $\mathrm{ld}\, N_P^{(w)} \approx 2.6$ [bit] , damit

(w) $U \approx \frac{1}{2.1}\, \mathrm{ld}\, Z$ für Entzifferung mittels Worthäufigkeiten

Die Shannon-Entropie der englischen wie auch der deutschen Sprache unter Heranziehung aller, auch grammatikalischer und semantischer Nebenbedingungen ist noch erheblich kleiner, man rechnet mit einem ungefähren Wert von $\mathrm{ld}\, N_P^{(*)} \approx 1.2$ [bit] und gewinnt damit die Unizitätslänge

($*$) $U \approx \frac{1}{3.5}\, \mathrm{ld}\, Z$ für Freistil-Entzifferung,

die auch in 12.6 angegeben ist.

Für einfache Substitution ist (12.1.1.1) $Z = 26!$, $\mathrm{ld}\, Z = 88.38$ und es ergeben sich für die Unizitätslänge die Werte 147, 74, 59, 42, 25, die durch die Erfahrung gut bestätigt werden. Die Situation ist für die englische, französische, deutsche, italienische, russische und verwandte indoeuropäische Sprachen ziemlich die gleiche.

A.5.2 Obschon *Shannon* durch seine Beschäftigung mit kryptologischen Fragen während des 2. Weltkriegs zu seiner Informationstheorie geführt wurde, hat diese in der dem Kommunikationstechniker geläufigen und ihn interessierenden Form keine kryptologischen Aspekte. Ihre praktische Bedeutung liegt hauptsächlich in der Steigerung der Übertragungsrate durch geeignete Codierung, bis hin zu einem Grenzwert, der nicht überschritten werden kann und der sich auf eine Nachricht P ohne jede Redundanz bezieht – also eine Nachricht P von k Zeichen mit der maximalen Unsicherheit $H(P) = k \cdot \mathrm{ld}\, N$.

Die obigen kryptologischen Ergebnisse lassen sich unmittelbar übertragen: Gewöhnliche natürliche Sprache ist redundant; ein Code für das einzelne Alphabetzeichen von Z_{26} läßt sich im Falle der englischen Sprache theoretisch reduzieren zu einer Codierung, die im Mittel ungefähr 1.20 [bit/char] erfordert – also etwa ein Viertel der Schranke von $\mathrm{ld}\, 26 = 4.70$ [bit/char]. Allerdings ist die Annäherung an diesen theoretischen Wert nur mit einigem Schaltaufwand erzielbar. Eine Huffman-Codierung der Einzelzeichen, die Binärwörter verschiedener, optimal gewählter Länge unter Beachtung der Rekonstruierbarkeit der Zeichenfuge benutzt – je seltener das Einzelzeichen, desto länger das Binärwort – reduziert die Übertragungsrate nur auf etwa 4.1 [*bit/char*] . Huffman-Codierung für m-gramme approximiert, wie oben gesehen, mit wachsendem m den Grenzwert nur langsam: 3.5 [bit/char] für Bigramme, 3.2 [bit/char] für Trigramme. In der Tat ist die bei gewöhnlichen

Sprachtexten erzielbare Komprimierung der Nachricht ohnehin nicht so groß, um besondere Aufwendungen zu rechtfertigen. Huffman-Tetragramm-Codierung sollte jedoch mit Hilfe spezieller Chips wirtschaftlich durchführbar sein.

Anders ist es bei Sprachübertragung und noch mehr so bei Bildübertragung, wo die erzielbare Komprimierung beträchtlich ist. Für diese Anwendungen kommt also der Binsenweisheit der Nach-Shannonschen Kryptologie „*Code-Komprimierung des Klartextes ist ein nützlicher Schritt zur Verbesserung der praktischen Sicherheit einer Chiffrierung*“ besondere Bedeutung zu.

A.6 Unmöglichkeit einer konstruktiven vollständigen Unordnung

Als in den zwanziger Jahren der Gebrauch individueller Schlüssel empfohlen wurde, schien ihre Herstellung kein besonderes Problem zu sein. Daß ein individueller Schlüssel eine Zufallsfolge einzelner Schlüsselzeichen sein sollte, leuchtete unmittelbar ein. Nach den Arbeiten von *Shannon* und insbesondere von *Chaitin* 1974 mußte man aber alle Versuche, eine echte Zufallsfolge algorithmisch zu fabrizieren, aufgeben; wenn man Algorithmen einsetzen wollte, mußte man auf echte Zufallsfolgen verzichten.

Im übrigen waren gerade ‚Pseudozufallsfolgen‘ mit langer Periode verdächtig, innere Gesetzmäßigkeiten zu haben, die kryptanalytischen Nutzen bringen könnten – wenn auch konkrete Beispiele fehlten und bis heute fehlen. Mehr und mehr mußten jedenfalls die für die Sicherheit der eigenen Kryptosysteme verantwortlichen Kryptologen Kopfschmerzen hinnehmen, während die eigentlichen Codebrecher sich in der Hoffnung auf unerwartete Einbrüche wiegen konnten.

Etwa um diese Zeit begann auch in der Mathematik eine einschlägige Entwicklung. So schrieben *H. Burkill* und *L. Mirsky* 1973

> *“There are numerous theorems in mathematics which assert, crudely speaking, that every system of a certain class possesses a large subsystem with a higher degree of organization than the original system.”*

Beispiele sind

(1) „Jeder Graph von n Knoten enthält entweder einen großen Teilgraph von k Knoten, der zusammenhängend ist, oder einen großen Teilgraph von k Knoten, der unzusammenhängend ist.“
(Ramsey-Zahl, z.B. $k = 6$ für $n = 102$, *F. P. Ramsey* 1930)

(2) „Jede beschränkte unendliche Folge komplexer Zahlen enthält eine konvergente unendliche Teilfolge.“ (*K. Weierstraß* 1865)

(3) „Wenn man die natürlichen Zahlen in zwei Klassen teilt, enthält mindestens eine eine beliebig lange arithmetische Reihe.“
(*Issai Schur* um 1925, *B. L. van der Waerden* 1927)

(4) „Jede partielle Ordnung von $n^2 + 1$ Elementen enthält entweder eine Kette der Länge $n + 1$ oder eine Menge von $n + 1$ nicht vergleichbaren Elementen.“ (*R. P. Dilworth* 1950)

(5) „Jede Folge von $n^2 + 1$ natürlichen Zahlen enthält entweder eine aufsteigend monotone oder eine absteigend monotone Teilfolge der Länge $n + 1$.“ (*P. Erdős, G. Szekeres* 1950)

Zwischen diesen und einigen anderen Beispielen schien zunächst kein Zusammenhang zu herrschen; besser gesagt, es wurde keiner bemerkt. Erst *P. Erdős* begann um 1950 mit einer Zusammenschau und gab ein allgemeines Theorem an, aus dem viele einzelne Ergebnisse durch Spezialisierung erhältlich waren. Unter dem Namen *'Ramsey Theory'* hat dies seit etwa 1970 zu vielen scharfsinnigen mathematischen Arbeiten über unordentliche Systeme mit ordentlichen Subsystemen geführt, beispielsweise 1975 zu einer Arbeit von *E. Szemerédi* mit dem Titel *'On sets of integers containing no k in arithmetic progression'* . Die prinzipielle Unmöglichkeit einer konstruktiven vollständigen Unordnung muß aber als eine Mahnung an die Kryptologie verstanden werden, beim Gebrauch von Pseudozufallsfolgen überaus vorsichtig zu sein – eine derzeit lediglich theoretische, aber nichtsdestoweniger ernstzunehmende und untersuchenswerte Warnung.

Marian Rejewski, polnischer Held der Entzifferung, drückte es 1978 (unter der stillschweigenden Voraussetzung der Konstruktivität) so aus:

> *“Whenever there is arbitrariness, there is also a certain regularity.”*

B Anhang: Kryptologische Geräte und Maschinen im Deutschen Museum München

(Auszug aus dem Führer durch die Ausstellung „Informatik“, Abschnitt 5.1 — Texte: Joachim Fischer)

1 **Chiffrierstäbchen in Holzschatulle** 1473
Satz mit 143 Stäbchen
Herkunft unbekannt; wohl 17. Jh.
Stifter: Mathematisch-Physikalische Sammlung des Staates Bayern

Mit Hilfe dieser Chiffrierstäbchen konnten polyalphabetische Chiffren „gelegt“ werden. Ein Satz enthält 143 Stäbchen, jedes Stäbchen ist auf zwei Seiten beschriftet.

2 **Chiffrierstäbchen in Holzschatulle** 1474
Satz mit 143 Stäbchen
Herkunft unbekannt; wohl 17. Jh.
Stifter: Mathematisch-Physikalische Sammlung des Staates Bayern

3 **Chiffrierscheibe** L 32/87;1
Messing, zum Teil versilbert; 18./19. Jh.
Stifter: Bayerisches Nationalmuseum, München (Leihgabe)

Die Chiffrierscheibe enthält neben den Alphabetzeichen auch häufig vorkommende Zeichengruppen des (deutschen) Klartextes, die Chiffren sind zweistellige Zahlen. Die Scheibe wurde vermutlich im diplomatischen Dienst in der ersten Hälfte des 19. Jh. gebraucht.

4 **Chiffrierscheibe** L 32/87;2
Messing, zum Teil versilbert; 18./19. Jh.
Stifter: Bayerisches Nationalmuseum, München (Leihgabe)

5 **Réglette St-Cyr** 88/132
(Nachbildung, 1987)

Schieber dieser Bauart waren im 19. Jh. in Gebrauch.

6 **Polyalphabetisches Chiffriergerät** 1994/99
Gerät in Uhrenform
Charles Wheatstone; nach 1867

Polyalphabetisches Chiffriergerät mit progressivem Schlüssel, der durch automatisches gegenseitiges Verdrehen der beiden Scheiben erzielt wird. Auf der Pariser Weltausstellung 1867 erstmals gezeigt.

7 **Chiffriergerät mit mehreren Schiebern** 87/736
(Nachbau, 1987)
Original im Besitz der Crypto AG, Zug
südamerikanisch; um 1920

Chiffriergerät in Schieberform, mit 7 verschiedenen Schiebern.

8 **Chiffriergerät M-94 der U.S.Army** 88/35

Chiffriergerät in zylindrischer Form, 25 gravierte Aluminiumscheiben von 35 mm Durchmesser. Die M-94 geht auf die Vorbilder von Jefferson und Bazeries zurück. Sie wurde 1922 unter dem Einfluß von Friedman für den Truppendienst eingeführt und war bis etwa 1942 in der amerikanischen Armee weithin in Gebrauch.

9 **Chiffriermaschine „Kryha“** 62797

A. v. Kryha, Berlin-Charlottenburg; um 1926
Stifter: A. v. Kryha, Berlin-Charlottenburg

Polyalphabetische Chiffriermaschine mit festem periodischen Schlüssel der Länge 442. Unregelmäßige Fortschaltung der Chiffratscheibe durch Rad mit wechselnder Zähnezahl. Trotz ihrer kryptologischen Mängel wurde die Maschine in viele Länder verkauft.

10 **Chiffrier-Zusatzgerät (Lochstreifenleser)** 87/1

Siemens & Halske T send 77 f
(als Zusatz zum Fernschreiber T 100 oder T 37 i)
Siemens & Halske, Wernerwerk München; 1964

Aus einem Lochstreifen mit Klartext und einem weiteren Lochstreifen, auf dem sich der fortlaufende Schlüssel befindet, wird ein dritter Lochstreifen erzeugt, der die Chiffre enthält. Zur Dechiffrierung wird auf die umgekehrte Weise aus der Chiffre und dem Schlüssel der Klartext hergestellt.

11 **Chiffrierfernschreibmaschine** 84/337;1-2

Siemens & Halske SFM T 52 e, Nr. 53260
Siemens & Halske, Wernerwerk Berlin, 1944
Stifter: Siemens AG, München

Chiffriermaschine für Fernschreibzeichen, im Jargon „Geheimschreiber“, britischer Deckname STURGEON. Erfinder: Ehrhard Roßberg, August Jipp und Eberhard Hettler. Deutsches Patent Nr. 615016, angemeldet am 18. Juli 1930. Durch zehn Stiftwalzen mit 73-,71-,69-,67-,65-,64-,61-,59-,53-,47-Teilung und unregelmäßig verteilten Stiften wird ein Schlüssel mit einer Periode von knapp 10 hoch 18 erzeugt. Fünf der Stiftwalzen steuern Vernam-Substitutionen des 5-Bit-Codes; die restlichen fünf bewirken Transpositionen der fünf Bits. Die Verteilung der Walzen auf diese Funktionen kann durch eine Stecktafel ausgewählt werden.

12 **Chiffrierfernschreibmaschine** 1988/81019

Schlüsselzusatz Lorenz SZ 42
C. Lorenz AG, Berlin, um 1943
Stifter: Standard Elektrik Lorenz AG, Stuttgart

Chiffriermaschine für Fernschreibzeichen, Britischer Deckname TUNNY.
Einsatzfeld: Heer-Armeehauptquartiere.
Durch zwölf Walzen mit 43-,47-,51-,53-,59-,37-,61-,41-,31-,29-,26-,23-Teilung und unregelmäßig verteilten Stiften wird ein Schlüssel mit hoher Periode erzeugt. Fünf Walzenpaare steuern Vernam-Substitutionen des 5-Bit-Codes; zwei Walzen dienen lediglich der unregelmäßigen Fortschaltung.
Die Chiffrierung der SZ 42 wurde von den Briten unter Einsatz der elektronischen COLOSSUS-Anlagen gebrochen.

13 **Rotor-Chiffriermaschine** 1993/522;1-2

Enigma, 3-Walzen-Ausführung, Holzgehäuse,
Nr. A 2178 K ; um 1938

Rotor-Chiffriermaschine mit Steckerfeld und Glühlampen-Anzeige, Einsatzfeld Heer („Wehrmacht-Enigma“). Umkehrwalze B, Walzen I (A 4200), II (A 102218), III (A 13947) in der Maschine, IV (A 7370), V (A 7692) im Zubehörkasten (eingestempelt „1939“).

14 **Rotor-Chiffriermaschine** 87/104

Enigma, 3-Walzen-Ausführung, Metallgehäuse,
Nr. A 02196/bac/44E ; 1944
Stifter: Siemens AG, Siemens Museum, München

Rotor-Chiffriermaschine mit Steckerfeld und Glühlampen-Anzeige, Einsatzfeld Heer/Luftwaffe („Wehrmacht-Enigma“). Neben der Umkehrwalze B sind nur die drei im Gerät befindlichen Walzen I, II, III (von ingesamt fünf), gestempelt A 02196/44E , vorhanden.

15 **Rotor-Chiffriermaschine** 84/584;1-3

Enigma, 4-Rotoren-Ausführung, Metallgehäuse mit Abdeckhaube, Nr. M 7972/jla/44; 1944

Rotor-Chiffriermaschine mit Glühlampenanzeige, Ausführung für die Marine. Dünne Umkehrwalze und insgesamt zehn Rotoren. Drei der vier Rotoren in der Maschine konnten aus den acht Rotoren I bis VIII ausgewählt werden, die vierte (ganz links) aus den sogenannten „Griechenwalzen“ β und γ . Im Zubehörkasten eingestempelt „Kommando der Marine-Station der Ostsee – Druckschriftenverwaltung“.

16 **Chiffriermaschine** 73800

Hagelin Cryptographer C-36, Nr. 702
Aktiebolaget Cryptoteknik, Stockholm, 1936
Stifter: Boris Hagelin, Zug

Bei allen C-Typen von Hagelin basiert die Chiffrierung auf der Verwendung von Schlüsselrädern unterschiedlicher Teilung. Im Gegensatz zu späteren Ausführungen sind bei der vorliegenden Maschine jedoch nur fünf Schlüsselräder mit 17-, 19-, 21-, 23- und 25-Teilung vorhanden, was eine Periodenlänge („Schlüssellänge“) von nur 3900225 ergibt. Für rein mechanisch arbeitende Maschinen bedeutete dies jedoch eine Pionierleistung.

17 **Chiffriermaschine** 87/180

Hagelin-Crypto CX-52, Serie D, Nr. 33244
Crypto AG, Zug; ab 1952
Stifter: Crypto AG, Zug

Chiffriermechanismus mit 6 Schlüsselrädern, deren Umfang jeweils verschieden geteilt ist; insgesamt steht ein Satz von 12 Rädern mit 25-, 26-, 29-, 31-, 34-, 37-, 38-, 41-, 42-, 43-, 46- und 47-Teilung zur Verfügung, von denen 6 ausgewählt werden können. Da (vom Faktor 2 abgesehen) die Teilungszahlen keinen gemeinsamen Teiler besitzen, ist die Periodenlänge sehr groß. Durch Zusatzgeräte zu diesem rein mechanischen Gerät ist die Bedienung als „elektrische Schreibmaschine“ möglich.

18 **Taschenchiffriermaschine** 87/42

Hagelin-Crypto CD-57, Nr. 3004061
Crypto AG, Zug; ab 1957
Stifter: Crypto AG, Zug

Chiffriergerät, das aufgrund seiner handlichen Größe vielfältigen Einsatz erlaubte; die Chiffrierung erfolgt wie bei der schweren Ausführung CX-52 mittels Schlüsselrädern verschiedener Teilung.

19 **Chiffriergerät mit Zusatz-Lochstreifengerät** 87/181;1-2

Hagelin-Crypto Type H-4605-3/X, Nr. 4.000.815 (Rotorgerät);
Hagelin-Cryptos Type PEH-72 antr. 2022a-2, Nr. 3.520.261 000000(Leser)
Crypto AG, Zug; hergestellt von 1963 bis 1965
Stifter: Crypto AG, Zug

Die Maschinen der „H-X“-Reihe sind autonome, elektrisch angetriebene 9-Rotor-Chiffriermaschinen für linienunabhängigen (‘off-line’) Lochstreifenbetrieb. Nach Eingabe eines Grundschlüssels von 25 Buchstaben ist das Gerät „voreingestellt“; die Grundschlüsselinformation bleibt gespeichert. Jede Nachricht, die chiffriert werden soll, benötigt darüber hinaus die Eingabe eines weiteren, 5 Buchstaben umfassenden sogenannten Spruchschlüssels.

Literatur

Gute amateurhafte Einführungen in die klassische Kryptologie geben:

Gaines, Helen F., Cryptanalysis. Dover, New York 1956

Smith, Laurence D., Cryptography. Dover, New York 1955

Millikin, Donald D., Elementary Cryptography and Cryptanalysis. New York 1943 (3. Aufl.)

Eine Einführung, die auch mathematisch orientierte Leser anspricht, ist:

Sinkov, Abraham, Elementary Cryptanalysis. Mathematical Association of America, Washington 1966

Dieses Buch ist von einem professionellen Kryptologen geschrieben und gibt sicher nicht dessen vollen Wissensstand wieder.

Ein Klassiker der Kryptanalyse ist:

Friedman, William F., Military Cryptanalysis. Part I, II, III, IV. Washington, 1938, 1938, 1938, 1942 *(neuerdings auch als Reprint erhältlich)*

Eine umfassende geschichtliche Darlegung der Kryptologie nach dem Stand der offenen Literatur von 1967 findet sich in:

Kahn, David, The Codebreakers. Macmillan, New York 1967

Dort findet man auch Hinweise auf spezielle, schwer zugängliche, insbesondere historische Literatur vor dem 19. Jahrhundert. Mit journalistischer Verve von einem Historiker geschrieben.

"Of primary importance for a knowledge of modern cryptology" (Kahn) ist der Artikel

Rohrbach, Hans, *Mathematische und Maschinelle Methoden beim Chiffrieren und Dechiffrieren.* FIAT Review of German Science, 1939–1946: Applied Mathematics, Vol. 3 Part I pp. 233–257, Wiesbaden: Office of Military Government for Germany, Field Information Agencies 1948

Nach 1967 bekanntgewordene Ergebnisse der englischen Entzifferer, einschließlich Einzelheiten über COLOSSUS, stehen in:

Bertrand, Gustave, Enigma ou la plus grande énigme de la guerre 1939–1945. Librairie Plon, Paris 1973

Winterbotham, Frederick W., The Ultra Secret. Weidenfeld and Nicolson, London 1974

Beesly, Patrick, Very Special Intelligence. Hamish Hamilton, London 1977

Lewin, Ronald, Ultra Goes to War. Hutchinson, London 1978

Johnson, B., The Secret War. Methuen, London 1978

Rohwer, J., Jäckel, E., Die Funkaufklärung und ihre Rolle im Zweiten Weltkrieg. Motorbuch-Verlag, Stuttgart 1979

Randell, Brian, The COLOSSUS. In: N. Metropolis et al., A History of Computing in the Twentieth Century. Academic Press, New York 1980

Hinsley, Francis H. et al., British Intelligence in the Second World War. Volumes I – IV, Cambridge University Press 1979–1988

Neuere aufschlußreiche Berichte über die ENIGMA sind:

Garliński, Józef, Intercept. The ENIGMA War. Scribner, New York 1980

Welchman, Gordon, The Hut Six Story: Breaking the Enigma Codes. McGraw-Hill, New York 1982

Kozaczuk, Władysław, ENIGMA. Arms and Armour Press, London 1984
Polnische Originalausgabe: 1979, deutsche Übersetzung Bernard und Graefe 1989.

Bloch, Gilbert, Enigma avant Ultra. Texte revisé. Selbstverlag, Paris 1985
Englische Übersetzung in Cryptologia XI (1987), XII (1988).

Kahn, David, Seizing the Enigma. Houghton-Mifflin, Boston 1991

Hinsley, Francis H., Stripp, Alan (eds.), Codebreakers. The inside story of Bletchley Park. Oxford University Press 1993 *(einschließlich COLOSSUS)*

Über statistische Methoden unterrichtet aus erster Hand:

Kullback, Solomon, Statistical Methods in Cryptanalysis. Aegean Park Press, Laguna Hills CAL 1976

Über kryptologische Geräte und Maschinen gibt Auskunft:

Türkel, Siegfried, Chiffrieren mit Geräten und Maschinen. Graz 1927

Deavours, C. A. und Kruh, L., Machine Cryptography and Modern Cryptanalysis. Artech House, Dedham MA 1985

Leicht lesbare Einführungen in die moderne Kryptologie sind:

Kippenhahn, Rudolf, Verschlüsselte Botschaften.
Rowohlt Verlag, Reinbek bei Hamburg 1997

Singh, Simon, Geheime Botschaften.
Carl Hanser Verlag, München 2000

Spezialwerke über moderne Kryptologie sind:

Brassard, G., Modern Cryptology. Lecture Notes in Computer Science, Vol. 325 , Springer, Berlin 1988

Beker, H. and Piper, F., Cipher Systems. Northwood Books, London 1982

Salomaa, Arto, Public-Key Cryptography. Springer, Berlin 1990

Die letzten beiden Bücher enthalten auch Details über die Kryptanalyse von Hagelin-Maschinen.

Schneier, Bruce, Applied Cryptography. Wiley, New York 1995 (2nd ed.)

Dieses Buch neueren Datums enthält Protokolle, Algorithmen und Quellcode in C.

Hoffman, Lance J. (ed.), Building in Big Brother. Springer, New York 1995

Ein Buch mit vielseitigen Beiträgen zur Grundrechte-Diskussion.

Goldreich, Oded, *Modern Cryptography, Probabilistic Proofs and Pseudo-randomness.* Springer, Berlin 1999

Ein typisches Buch für den modernen Teil der wissenschaftlichen Kryptologie.

Weitere Literatur:

Horster, P., Kryptologie. BI, Mannheim 1985

Beutelspacher, A., Kryptologie. Vieweg, Braunschweig 1994 (4. Aufl.)

Die mathematischen Hintergründe sind vorzüglich zu finden in:

Forster, Otto, Algorithmische Zahlentheorie. Vieweg, Braunschweig 1996

Von den Spezialzeitschriften sei erwähnt:

Cryptologia. A Quarterly Journal Devoted to Cryptology. Editors: David Kahn, Louis Kruh, Cipher A. Deavours, Brian J. Winkel, Greg Mellen. ISSN 0161-1194. Terre Haute, Indiana, USA.

Journal of Cryptology. The Journal of the International Association for Cryptologic Research. Editor-in-Chief: Joan Feigenbaum. ISSN 0933-2790. Springer, New York, USA.

Unter dem Titel Advances in Cryptology *erscheinen die Tagungsberichte der alljährlich stattfindenden* International Cryptology Conference (CRYPTO), International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT) *und* International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), *unterstützt von der* International Association for Cryptologic Research (IACR), *in der Reihe* Lecture Notes in Computer Science, Springer, Berlin

Hauptsächlich für Historiker interessant sind die Werke von

Breithaupt 1737, Hindenburg 1795, 1796; Andres 1799; Klüber 1809; Lindenfels 1819; Vesin de Romanini 1838, 1844; Kasiski 1863; Myer 1866; Koehl 1876; Fleißner von Wostrowitz 1881; Kerckhoffs 1883; Josse 1885; de Viaris 1888, 1893; Valério 1892; Carmona 1894; Gioppi di Türkheim 1897; Bazeries 1901; Myszkowski 1902; Delastelle 1902; Meister 1902, 1906; Schneickert 1900, 1905, 1913; Hitt 1916; Langie 1918; Friedman 1918, 1922, 1924, 1925; Givierge 1925; Lange & Soudart 1925; Sacco 1925, 1947; Figl 1926; Gyldén 1931; Yardley 1931; Ohaver 1933; Baudouin 1939; d'Agapayeff 1939; Pratt 1939; Eyraud 1953; Weiss 1956; Muller 1971; Konheim 1981; Meyer-Matyas 1982.

Eine ausführliche Bibliographie bietet:

Shulman, D., An Annotated Bibliography of Cryptography. Garland, New York 1976.

Die Werke von Hitt, Kullback, Friedman, Sacco, Gyldén, Givierge, Lange &Soudart, Ohaver, Langie *sind als Reprints erhältlich von AEGEAN PARK PRESS, P.O.B. 2837, Laguna Hills, Calif. 92654-0837, USA.*

Die englischsprachige Ausgabe des vorliegenden Buches ist unter dem Titel „Decrypted Secrets“ in zweiter Auflage bei Springer, Berlin 2000 erschienen.

Namen- und Sachverzeichnis

Lösung zum zweiten Cryptoquip von Abb. 87:

I=m. Einstieg mit Suche nach Mustern *1211234* (KRKKRLH) und *53675* (ULZIU). Unter den etwa ein Dutzend Möglichkeiten sind nur einige wenige nicht allzu ausgefallen. Von diesen führen /peppery/ und nachfolgend (für *5*r*6*m*5*) /aroma/ schnell zum Ziel:

KRKKRLH	PLRUI	OZGK	AYMMGORA	U	LYPQ,	QRUAH	ULZIU
peppery	re m	p	e		r ,	e y	r m
peppery	ream	o p	e	a	r ,	ea y	aroma
peppery	cream	soup	use	a	r c ,	ea y	aroma
peppery	cream	soup	i use	a	rich,	hea y	aroma
peppery	cream	soup	di used	a	rich,	heady	aroma
peppery	cream	soup	diffused	a	rich,	heady	aroma

Bildquellenverzeichnis

Kahn, David, *The Codebreakers*. Macmillan, New York 1967:
Abb. 1, 4, 5, 12, 23, 30, 31, 33, 34, 35, 36, 37, 38, 40, 57

Smith, Laurence Dwight, *Cryptography*. Dover, New York 1955:
Abb. 3, 16, 24, 53

Bayerische Staatsbibliothek München
Abb. 10, 52

Lange, André and E.-A. Soudart, *Traité de cryptographie*. Paris 1925:
Abb. 26

Crypto AG, Zug, Schweiz:
Abb. 48, 54, 55, 60, 61, 62, 64, 65, Farbtafeln L, O, P

Deavours, Cipher A. and Kruh, Louis, *Machine Cryptography and Modern Cryptanalysis*. Artech House, Dedham, MA 1985:
Abb. 63, 66, 67, 68

SiemensForum München:
Abb. 70

Public Record Office, London:
Abb. 143

FRA, Bromma, Schweden:
Abb. 145

Deutsches Museum (Reinhard Krause), München:
Farbtafeln A, B, C, D, F, G, I, K, N, Q

Russell, Francis, *The Secret War*. Time-Life Books, Chicago, IL 1981:
Farbtafeln E, H, M